

AUTOMÁTICA E INSTRUMENTACIÓN.com

www.automaticaeinstrumentacion.com

TECNOLOGÍA

La protección de infraestructuras críticas requiere un enfoque colaborativo y adaptados a los nuevos peligros

AMENAZAS CIBERNÉTICAS EN LA INDUSTRIA: UN RETO PARA LA CIBERSEGURIDAD OT

Pág. 36



ENTREVISTA

Jennifer Prgesa

Senior Product Manager en Honeywell Connected Enterprise

“Los simuladores son el mejor sustituto para operaciones reales en un entorno seguro”

Pág. 14



SECTOR

IA y ciudad: el amanecer de una nueva era en el urbanismo

Pág. 20



INFORME

Los cobots redefinen la colaboración en la industria

Pág. 26

Power Reliability, un sinfín de posibilidades



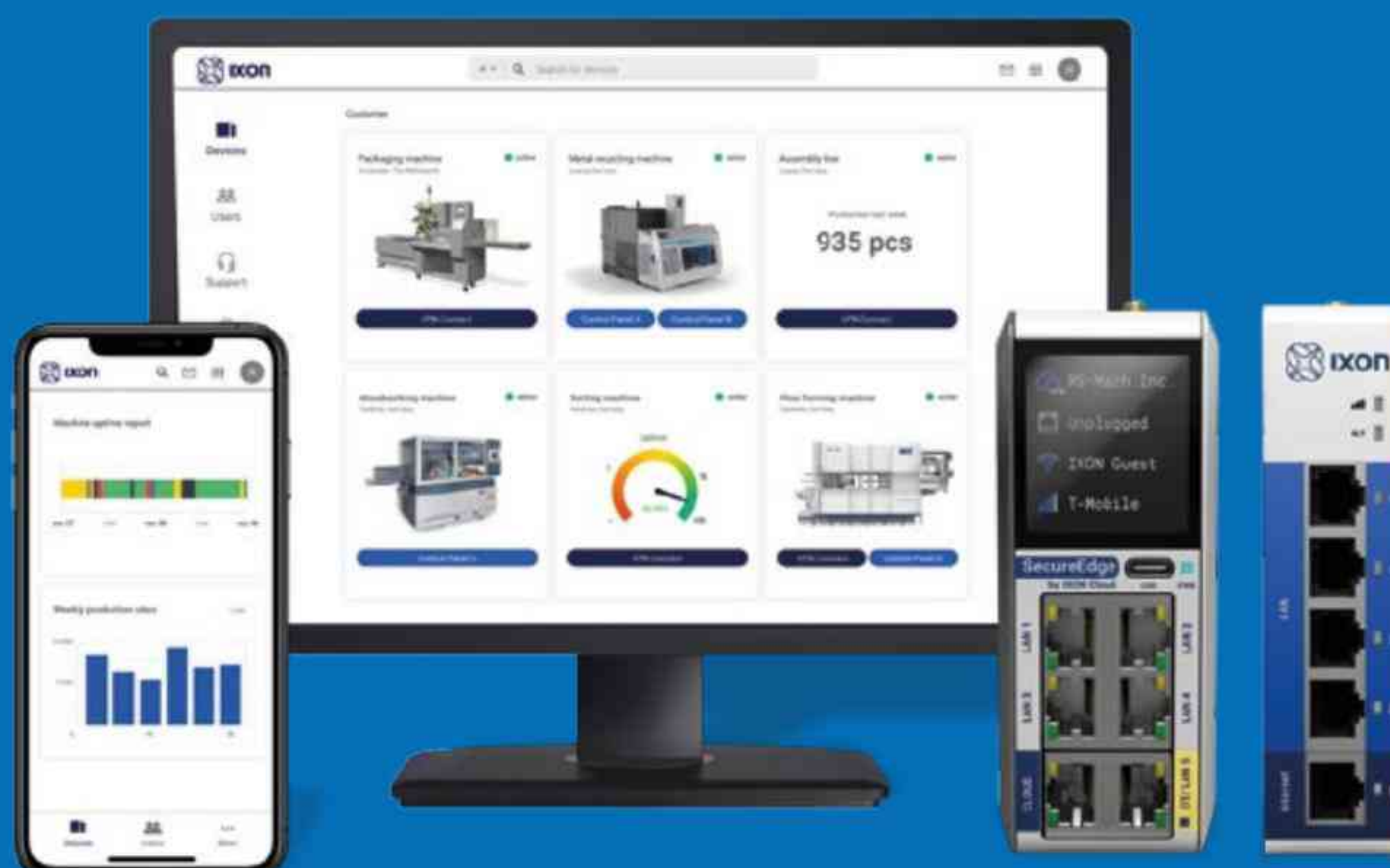
**PHOENIX
CONTACT**



Acceso remoto VPN gratuito e ilimitado para fabricantes de maquinaria

IXON la primera plataforma IIoT sin código del mundo, ofrece una solución amigable para todas sus necesidades de mantenimiento y servicio remoto: desde el hardware hasta la nube.

Su socio clave en ciberseguridad para máquinas.



IXON puede transformar sus servicios como fabricante de maquinaria



Máquinas conectadas y ciberseguridad

Red mundial de servidores distribuidos en 17 centros de datos.
Certificaciones ISO.



Acceso remoto seguro

Con IXON Cloud podrá proporcionar soporte sin desplazarse al lugar donde está la máquina.



Solución IIoT integrada

Diseñada para fabricantes de maquinaria, integradores de sistemas y automatización.



Conocimiento profundo de los datos de las máquinas

Cree valor añadido a partir de los datos históricos de la máquina.



Reduzca el tiempo de inactividad de las máquinas

El equipo experto de IXON está siempre a su disposición para brindarle asistencia técnica.



Secure EdgePro

El router SecureEdge Pro de IXON ofrece aislamiento físico de la red OT de fábrica, de la red de IT e Internet.



Aumente sus ingresos

Incrementa las ventas de sus máquinas con servicios recurrentes.



Diferénciese de sus competidores

Cree un portal de acceso para clientes y planifique e implemente una estrategia de servicio digital.

¿Quiere ampliar información?

Contacte con RTC

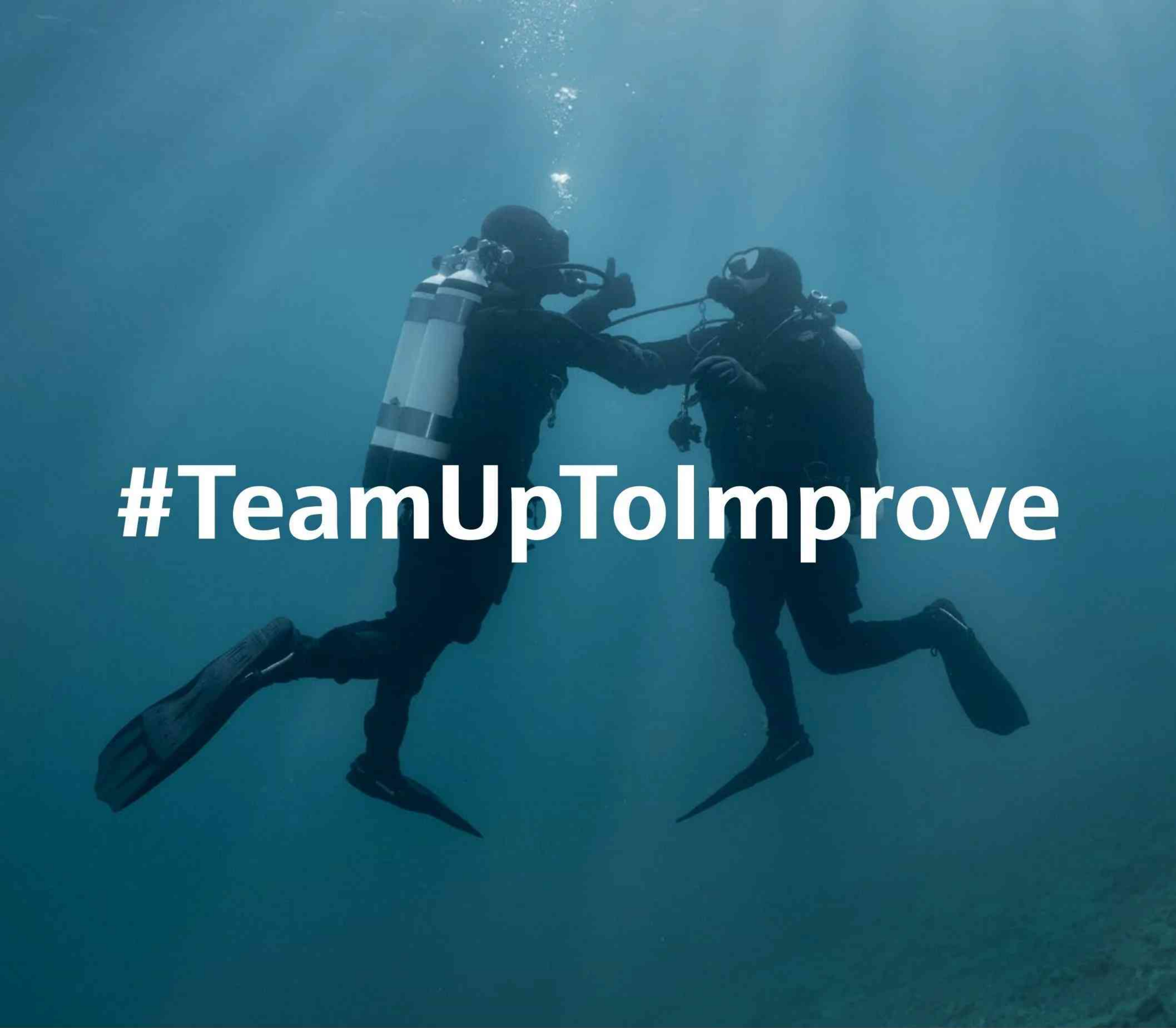
✉ rtc@grupcarol.com

En RTC somos partners de IXON y distribuidores de material eléctrico y automatización industrial. Nuestro equipo técnico se encuentra a su disposición.

Visite nuestro sitio web o escanee el código QR para ampliar información:

www.rtcautomatismos.com





#TeamUpToImprove

**La mejora de procesos
es como bucear.**

Necesitas un socio fiable
con el que contar.

Al igual que los atletas confían en sus compañeros de equipo, sabemos que la asociación con nuestros clientes aporta el mismo nivel de apoyo y fiabilidad en el ámbito de la producción. Juntos podemos superar los retos y alcanzar un objetivo común; optimizar los procesos en lo que respecta a la eficiencia económica, la seguridad y la protección del medio ambiente. Mejoremos juntos.



Más información...
www.es.endress.com

Endress+Hauser 
People for Process Automation



Power Reliability: un sinfín de posibilidades

Soluciones para la disponibilidad de la planta

La creciente electrificación, interconexión y automatización de los sectores aumenta la necesidad de soluciones fiables de suministro y supervisión de la energía.

Para un funcionamiento eficaz, se necesitan soluciones de suministro fiables que dispongan de protección contra sobretensiones, fuente de alimentación, protección de equipos y monitorización de la energía con la tecnología de medición adecuada. Phoenix Contact ofrece todos los servicios, desde la selección y la implantación hasta el apoyo durante el funcionamiento.

Más información:

<https://www.phoenixcontact.com/power-reliability>

EDITORIAL

5 Innovación y ciberseguridad, pilares del futuro industrial

TIEMPO REAL

6 Noticias de actualidad

OPINIÓN

10 Fabricación inteligente 2024 en España, por Antoni Rovira

PAPER AER

12 Visión artificial

ENTREVISTA

14 Jennifer Prgesa, Senior Product Manager en Honeywell Connected Enterprise
“Los simuladores son el mejor sustituto para operaciones reales en un entorno seguro”

SELECCIÓN DEL MES

16 Los Delta D-Bots ganan el ‘Red Dot: Best of the Best’ 2024 por su diseño y creatividad de vanguardia
18 Ixon como plataforma IIOT para fabricantes de maquinaria

SECTOR

20 IA y ciudad: el amanecer de una nueva era en el urbanismo

INFORME

26 Los cobots redefinen la colaboración en la industria

TECNOLOGÍA

36 Amenazas cibernéticas en la industria: un reto para la ciberseguridad OT
50 Gestión eficiente de la conectividad, clave del éxito para la digitalización
54 ¿Y si redefinimos la triada de ciberseguridad en sistemas OT?
60 Consejos en el desarrollo de robots en la automatización y optimización de procesos

TECNOMARKET

62 Novedades de producto

INNOVACIÓN Y CIBERSEGURIDAD, PILARES DEL FUTURO INDUSTRIAL

En la intersección entre la transformación digital y la seguridad, la ciberseguridad emerge como un aspecto clave para el desarrollo de la industria moderna. En este número, analizamos cómo las nuevas tecnologías no solo están mejorando la eficiencia operativa, sino que también están redefiniendo la forma en que las empresas protegen sus infraestructuras críticas frente a amenazas cada vez más sofisticadas.

LA CIBERSEGURIDAD ES AHORA UN PILAR CLAVE DE LA TRANSFORMACIÓN INDUSTRIAL, ASEGURANDO LA PROTECCIÓN DE INFRAESTRUCTURAS Y LA CONTINUIDAD OPERATIVA

La automatización, liderada entre otras tecnologías por la incorporación de robots colaborativos (cobots), ha revolucionado la manera en que operan las plantas industriales. Estos robots trabajan junto a los humanos, haciendo los procesos más seguros y eficientes, pero su integración también exige un nivel de protección adecuado en un entorno de creciente conectividad.

Es aquí donde la ciberseguridad se convierte en un pilar fundamental. La convergencia entre las redes IT y

OT ha ampliado las superficies de ataque, exponiendo a las infraestructuras industriales a nuevos riesgos. En este sentido, la segmentación de redes y el control granular de los protocolos industriales se han convertido en estrategias imprescindibles para proteger los sistemas de control, manteniendo la continuidad de las operaciones y evitando paradas no planificadas.

Paralelamente, la inteligencia artificial está jugando un papel crucial en esta transformación. Herramientas avanzadas basadas en IA están optimizando la seguridad de las redes y detectando patrones de comportamiento anómalos, permitiendo que las empresas sean más proactivas ante ciberataques. Esta tecnología, aplicada también en ámbitos como la visión artificial, no solo mejora la precisión y el control de calidad en la producción, sino que también anticipa posibles problemas en tiempo real.

Además, la IA comienza a abrir nuevos horizontes en áreas como el urbanismo y la planificación de infraestructuras. Aunque este tema puede parecer alejado de la ciberseguridad, lo cierto es que los datos recogidos y procesados para mejorar las ciudades del futuro necesitarán un nivel de protección acorde a su relevancia. El equilibrio entre progreso y seguridad será crucial para garantizar un crecimiento sostenible y seguro.

En resumen, este número subraya cómo la innovación y la ciberseguridad son los cimientos sobre los cuales la industria debe construir su futuro. Las empresas no solo están adoptando tecnologías para mejorar su competitividad, sino que están invirtiendo en soluciones que les permiten proteger su infraestructura y su información. En este contexto, la seguridad y la eficiencia ya no son aspectos separados, sino que van de la mano en la configuración de un entorno industrial más resiliente y confiable.

AUTOMÁTICA E INSTRUMENTACIÓN

www.automatacaeinstrumentacion.com

[@automatica_](https://x.com/automatica_) [/automatacaeinstrumentacion](https://facebook.com/automatacaeinstrumentacion) [Automatica e Instrumentación](https://in.linkedin.com/company/automatacaeinstrumentacion)

DIRECTORA EDITORIAL

Mónica Alonso
monica.alonso@automatacaeinstrumentacion.com

REDACCIÓN

Óliver Miranda
oliver.miranda@automatacaeinstrumentacion.com
Rebeca Santamarta
David Borja Peinado

CONSEJO ASESOR

Juan Manuel Ferrer (Coordinador), José Bielza, Francisco Díaz Andreu, César de Prada Moraga, José Ignacio Armesto y David Jiménez

CEA (Comité Español de Automática)

Carlos Balaguer (Presidente), Guillermo Ojea (Vicepresidente), Ramon Costa (Secretario)

DIRECTOR COMERCIAL DE ÁREA

Eusebio Albert
eusebio.albert@versysediciones.com

Ejecutivos de cuentas

Víctor Bernabeu
vbernabeu@automatacaeinstrumentacion.com
María Jesús Mora
mjesus.mora@automatacaeinstrumentacion.com
Asesor Comercial
Francisco Márquez

MAQUETACIÓN. Manuel Beviá

IMPRIME: Gama Color
DEPÓSITO LEGAL: M-3852-2014
ISSN: 0213-3113
ISSN (internet): 1989-0176

CEO

José Manuel Marcos
Franco de Sarabia

DIRECTORA OPERACIONES

Esther Crespo

DIRECTOR DE EXPANSIÓN Y DESARROLLO

José Manuel Marcos de Juanes

versys
EDICIONES TÉCNICAS

Versys Ediciones Técnicas S.L.

C/ Invierno, 17. 28850 - Torrejón de Ardoz (Madrid)
Tel.: 912 972 000
administracion@versysediciones.com

COPYRIGHT. Versys Ediciones Técnicas, S. L.

La suscripción a esta publicación autoriza el uso exclusivo y personal de la misma por parte del suscriptor. Cualquier otra reproducción, distribución, comunicación pública o transformación de esta publicación sólo puede ser realizada con la autorización de sus titulares. En particular, la Editorial, a los efectos previstos en el art. 32.1 párrafo 2 del vigente TRLPI, se opone expresamente a que cualquier fragmento de esta obra sea utilizado para la realización de resúmenes de prensa, salvo que cuente con la autorización específica. Dirijase a CEDRO (Centro Español de Derechos Reprográficos) si necesita fotocopiar, escanear, distribuir o poner a disposición de otros usuarios algún fragmento de esta obra, o si quiere utilizarla para elaborar resúmenes de prensa (www.conlicencia.com; 917021970 / 932720447). Las opiniones y conceptos vertidos en los artículos firmados lo son exclusivamente de sus autores, sin que la revista los comparta necesariamente.



En Europa crece un 9% hasta alcanzar un nuevo máximo de 92.393 unidades

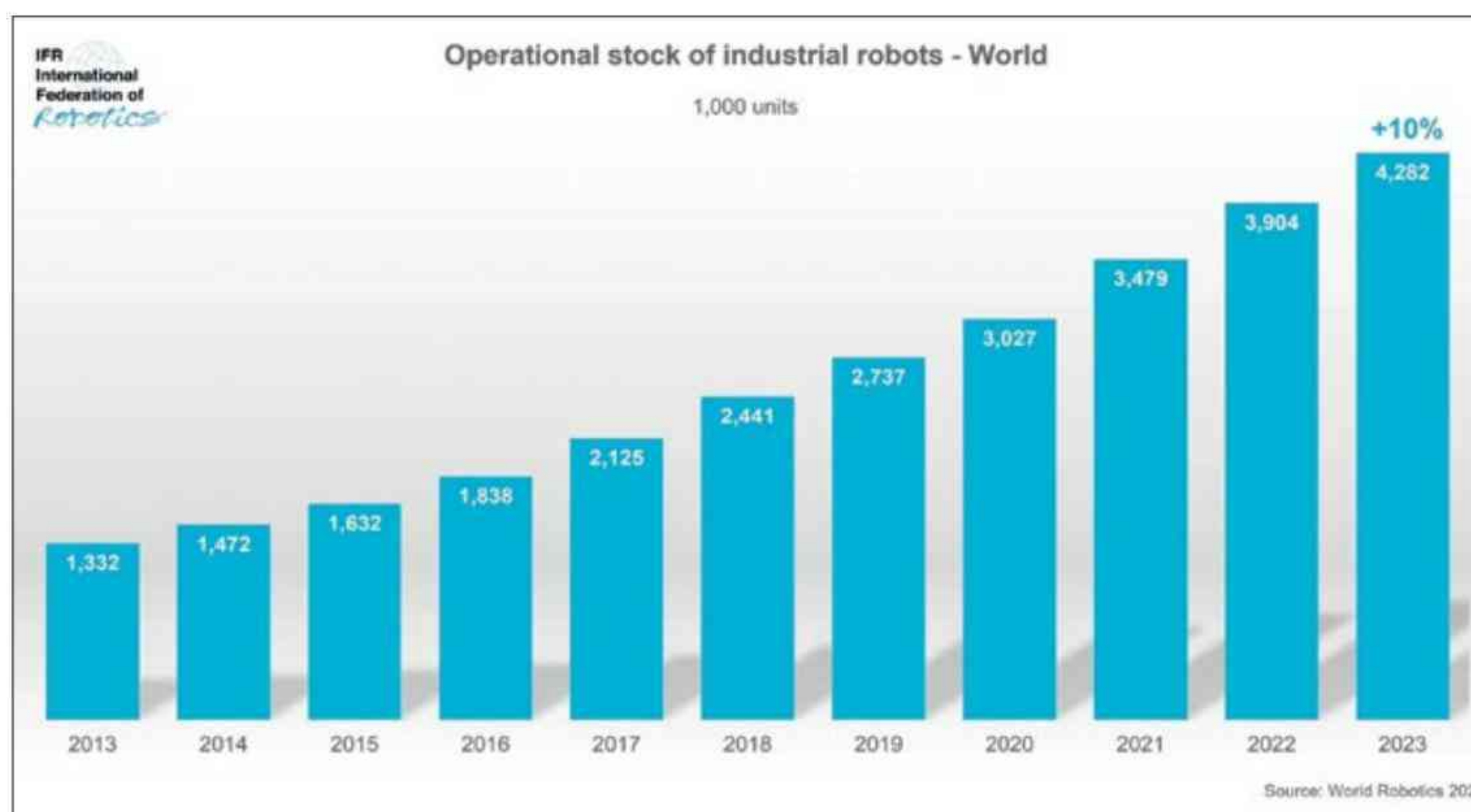
LA INSTALACIÓN DE ROBOTS EN FÁBRICAS AUMENTA UN 10% EN TODO EL MUNDO EN 2023

La Federación Internacional de Robótica ha presentado su nuevo informe World Robotics en el que ha registrado 4.281.585 unidades operando en fábricas de todo el mundo, lo que supone un aumento del 10%. Las instalaciones anuales superaron el medio millón de unidades por tercer año consecutivo. Por regiones, el 70% de todos los robots recién implementados en 2023 se instalaron en Asia, el 17% en Europa y el 10% en la América.

“Las nuevas estadísticas de World Robotics muestran un máximo histórico en el número de robots industriales que automatizan la producción en todo el mundo”, dice Marina Bill, presidenta de la Federación Internacional de Robótica. “La cifra anual de instalación de 541.302 unidades en 2023 es la segunda más alta de la historia. Es solo un 2% más baja que el récord de 552.946 unidades instaladas en 2022”.

Europa

Las instalaciones de robots industriales en Europa aumentaron un 9% hasta alcanzar un nuevo máximo de 92.393 unidades. En total, el 80% de las instalaciones en 2023 se podrían atribuir a destinos de la Unión Europea (73.534 unidades, un 2% más). Los proyectos retrasados se completaron y los atrasos se eliminaron en 2023. La demanda de robots en la región también se benefició de la tendencia de la deslocalización. En 2023, el crecimiento estuvo fuertemente impulsado por la inversión de la industria automotriz en países tradicionalmente fuertes en la fabricación de automóviles, como España (5.053 unidades, +31%), pero también en mercados más pequeños como Eslovaquia (2.174 unidades, +48%) o Hungría (1.657 unidades, +31%). Las instalaciones en Alemania, el mayor mercado europeo y el único europeo entre los cinco primeros del mundo, aumentaron un 7% hasta las 28.355 unidades. Las instalaciones en el segundo mercado europeo más grande, Italia, disminuyeron un 9% hasta las 10.412 unidades. El tercer mercado europeo más grande, Francia, bajó un 13%, instalando 6.386 unidades.



Los robots operativos en todo el mundo superan los 4 millones.

Asia

China es, con diferencia, el mercado más grande del mundo. Los 276.288 robots industriales instalados en 2023 representan el 51% de las instalaciones mundiales.

Le sigue Japón, como segundo mercado mundial más grande de robots industriales. Las instalaciones de robots alcanzaron las 46.106 unidades en 2023, un 9% menos.

El mercado en la República de Corea tiene una tendencia lateral: las instalaciones alcanzaron las 31.444 unidades en 2023, un 1% menos interanual. El país fue el cuarto mercado de robots más grande del mundo en términos de instalaciones anuales, después de Estados Unidos, Japón y China.

Por su parte, India es una de las economías asiáticas emergentes de más rápido crecimiento. Las instalaciones de robots aumentaron un 59% a 8.510 unidades en 2023, un nuevo máximo.

En el Reino Unido, las instalaciones de robots industriales aumentaron un 51% a 3.830 unidades en 2023. La inversión fue impulsada por las instalaciones en la industria automotriz, principalmente para tareas de ensamblaje.

América

Las instalaciones de robots en América superaron las 50.000 unidades por tercer año consecutivo: se instalaron

55.389 unidades en 2023, solo un 1% por debajo del nivel récord alcanzado en 2022.

Estados Unidos, el mercado regional más grande, representó el 68% de las instalaciones en esta región en 2023. Las instalaciones de robots bajaron un 5% a 37.587, esta es la tercera cifra récord más alta después de 2022 y 2018.

Perspectivas

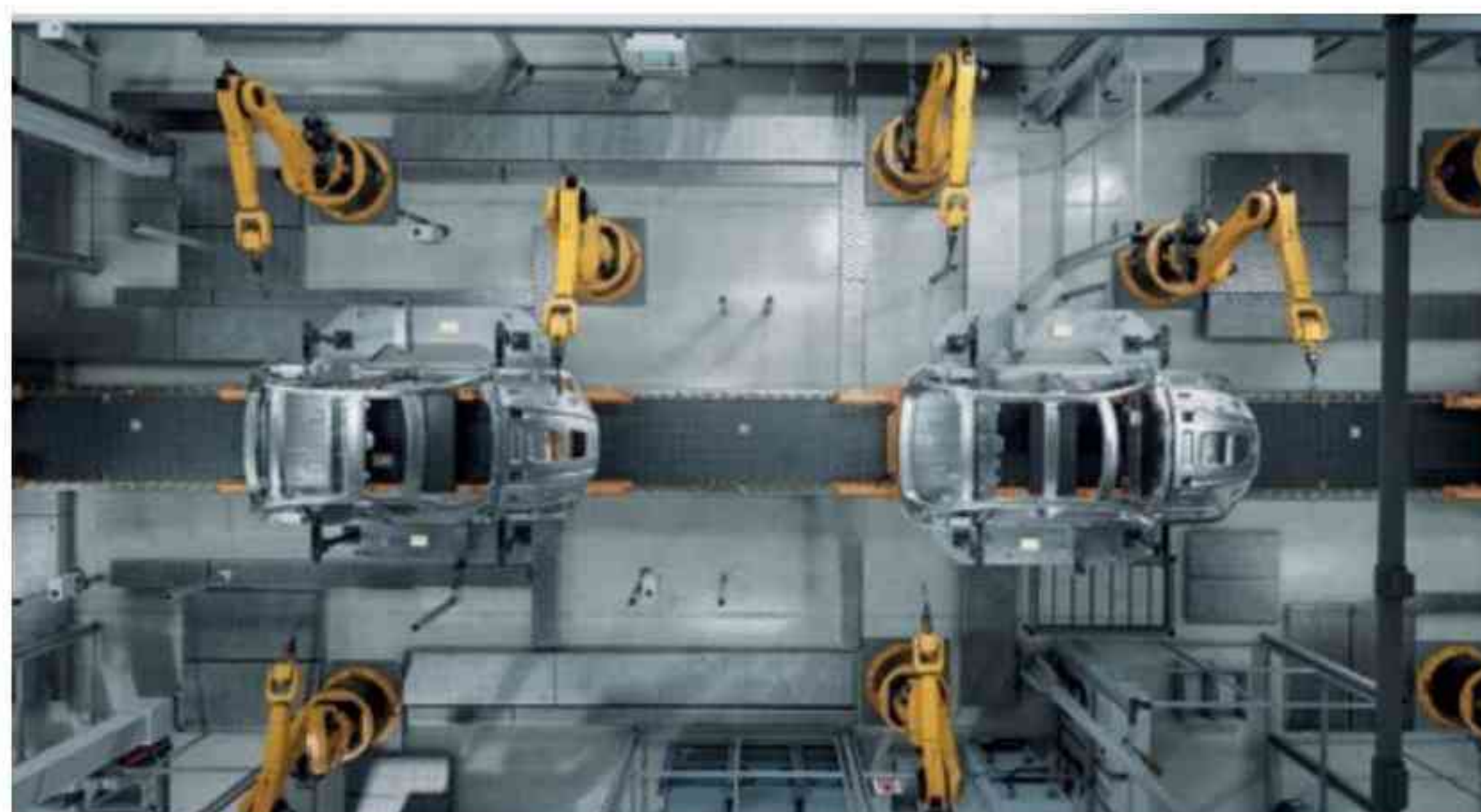
La OCDE espera que el crecimiento mundial se estabilice, pero los obstáculos geopolíticos siguen considerándose un importante factor de riesgo e incertidumbre. Las crisis recientes han aumentado la conciencia política sobre la capacidad de producción nacional en industrias estratégicas. La automatización permite a los fabricantes localizar la producción en economías desarrolladas sin sacrificar la eficiencia de los costos.

Para 2024, la crisis económica mundial habrá tocado fondo. Se espera que las instalaciones mundiales de robots se estabilicen en 541.000 unidades. Se prevé que el crecimiento se acelere en 2025 y continúe en 2026 y 2027. No hay señales de que la tendencia general de crecimiento a largo plazo vaya a terminar en el futuro cercano.

BITMAKERS CUMPLE 40 AÑOS APOSTANDO POR LA INNOVACIÓN EN AUTOMATIZACIÓN INDUSTRIAL

Bitmakers celebra este año su 40 aniversario como referente en soluciones de automatización industrial. Desde su fundación, experimenta un crecimiento constante, y cuenta en la actualidad con un equipo de más de 85 personas y 10 delegaciones en toda España.

La compañía es el distribuidor oficial y exclusivo en España de Keyence, empresa japonesa de fabricación de equipos de automatización industrial y reconocida por su innovación y tecnología avanzada, ofreciendo soluciones en detección, trazabilidad, inspección por visión artificial, medición sin contacto, seguridad industrial, control de estática y metrología dimensional.



■ **Desde 1984, la empresa ha experimentado un crecimiento constante, en la actualidad cuenta con más de 85 personas y 10 delegaciones en toda España.**

Desde 1984, está comprometida con la satisfacción del cliente, optimizando y mejorando la competitividad de los procesos productivos de sus clientes. Además, ha sido reconocida por su solvencia y crecimiento, siendo seleccionada por Cepyme como

una de las empresas destacadas en crecimiento en España.

Con una amplia gama de productos de Keyence, ofrece soporte especializado a sus clientes, ayudándoles a resolver sus necesidades de automatización con soluciones innovadoras y fiables. Su modelo de negocio y de trabajo le ha permitido lograr el éxito a lo largo de los años.

Además, mantiene como objetivo no dejar nunca de evolucionar y por ello continúa actuando en el presente con una visión de futuro, reafirmando su posición como socio de confianza en automatización industrial.

Ael

Nidec

Drives

Soluciones de movimiento rentables y escalables

Fácil integración de la línea

Máxima calidad

Alta precisión

CONTROL
TECHNIQUES

Celebrada en Hamburgo (Alemania) del 3 al 6 de septiembre

RITTAL Y EPLAN PARTICIPAN EN LA SHIPBUILDING, MACHINERY & MARINE TECHNOLOGY 2024



■ Por primera vez, Rittal presentó en el SMM la gama de refrigeradores Blue e+ dynamic que han sido probados y certificados con éxito por DNV para aplicaciones marinas.

Rittal y Eplan acudieron a la feria Shipbuilding, Machinery & Marine Technology, que se celebró del 3 al 6 de septiembre en Hamburgo (Alemania). Ambas compañías llevaron a este encuentro sus respectivas actividades y compromisos en relación con la transformación de la industria: los visitantes pudieron descubrir y conocer de cerca las últimas soluciones para lograr la coherencia de datos en el diseño, la planificación, la ingeniería y la fabricación de equipos de construcción naval.

El estándar de ingeniería para la construcción naval y las aplicaciones en alta mar, portuarias y de infraestructuras Eplan mostró soluciones integrales para la tecnología operativa completa de los buques. Las empresas pueden beneficiarse de un único sistema de establecimiento de estándares para diversas áreas dentro de la industria marítima: La plataforma Eplan ofrece diseño, planificación, presentación y documentación acreditados para el sector marítimo de ingeniería eléctrica, tecnología de automatización, ingeniería de procesos,

tecnología de climatización y ventilación, neumática e hidráulica, junto con la gestión de proyectos, cables y equipos, y todo ello con una arquitectura de sistema basada en datos. De esta manera, se puede crear un gemelo digital completamente funcional, desde componentes individuales hasta el barco completo. Lo más destacado del stand fue la demostración de un flujo de trabajo de Module Type Package (MTP) independiente del fabricante, desde el diseño, la planificación y la ingeniería hasta la automatización sin interrupciones ni inconsistencias en los datos. Esto se demuestra con el MTP Designer de Phoenix Contact y un ejemplo real de un sistema de agua de sentina de GEA. Rittal presentó por primera vez su gama de refrigeradores probadas con éxito por DNV (Blue e+ Dynamic) para aplicaciones marítimas. La compañía ha desarrollado aún más sus soluciones de refrigeración, específicamente para cargas dinámicas en alta mar. Además de las pruebas habituales de compatibilidad EMC para barcos, también se probó la resistencia a las vibraciones y el funcionamiento seguro de los refrigeradores cuando están inclinados. La certificación DNV significa que estas unidades operan de manera efectiva y se enfrían de manera segura y confiable, incluso bajo fuertes cargas dinámicas.

Ael

Cursos Siemens SITRAIN

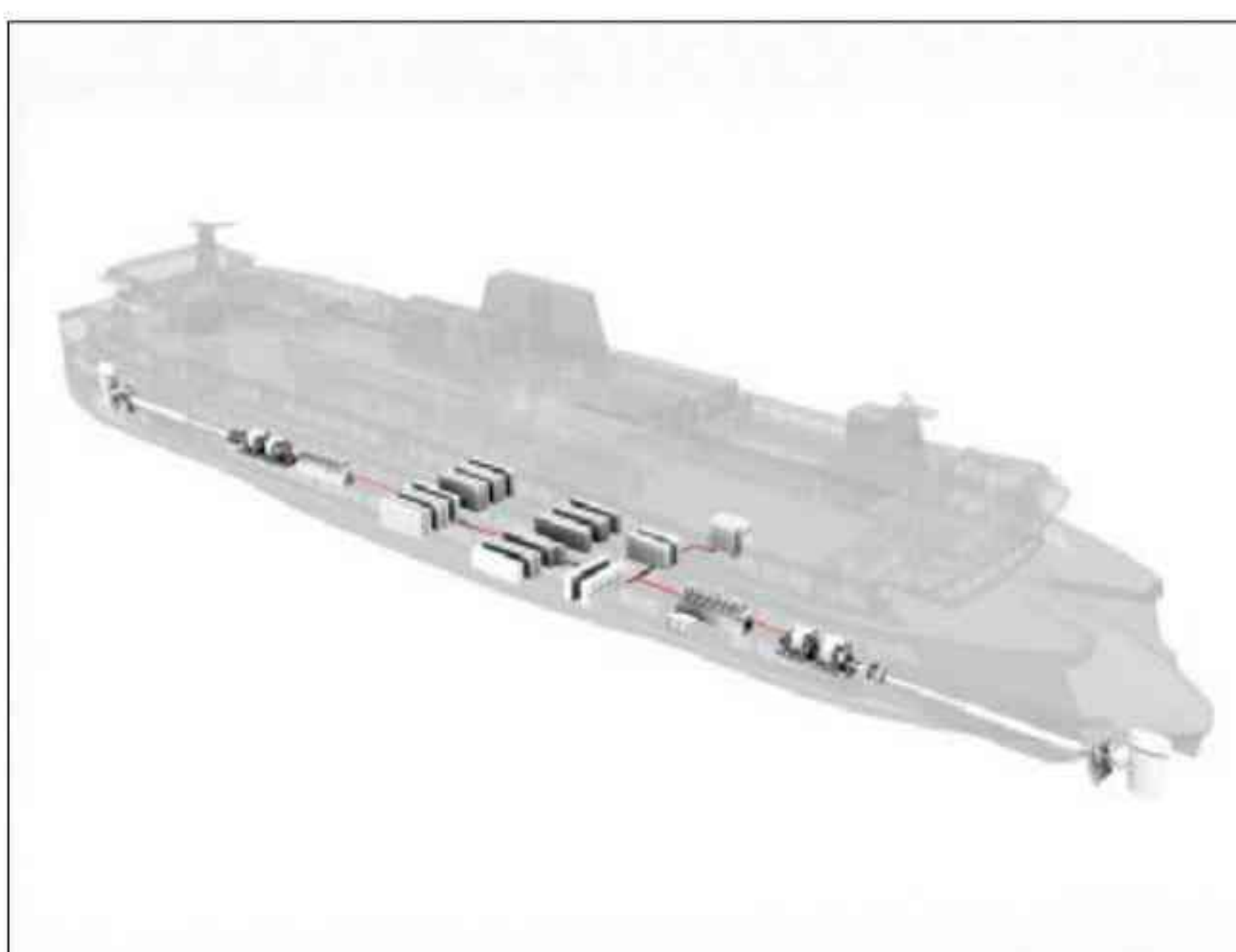
Fecha inicio	Fecha fin	Duración	Nombre del curso	Localidad
14/10/24	18/10/24	5 días - 35 horas	TIA Portal Programación 1	Valencia

Más información en: www.siemens.es/sitrain sitrain.es@siemens.com

ABB ELEGIDO PROVEEDOR ÚNICO DE PROPULSIÓN DE WASHINGTON STATE FERRIES

Washington State Ferries ha nombrado a ABB como proveedor único de propulsión (PSSV) para sus nuevos ferris híbridos eléctricos de 160 automóviles, un proyecto que marca un hito importante en la evolución del transporte marítimo sostenible en los EEUU. ABB desempeña un papel fundamental en el desarrollo y la entrega de los cinco buques de nueva construcción.

Como PSSV, la compañía suministrará sistemas completos de propulsión eléctrica híbrida que incluyen la solución de distribución de energía Onboard DC Grid, almacenamiento de energía, gestión avanzada de la energía y la automatización del buque. El paquete de propulsión está diseñado para mejorar la eficiencia operativa, ayudar a reducir las emisiones y garantizar un rendimiento



■ ABB suministrará sistemas completos de propulsión eléctrica híbrida.

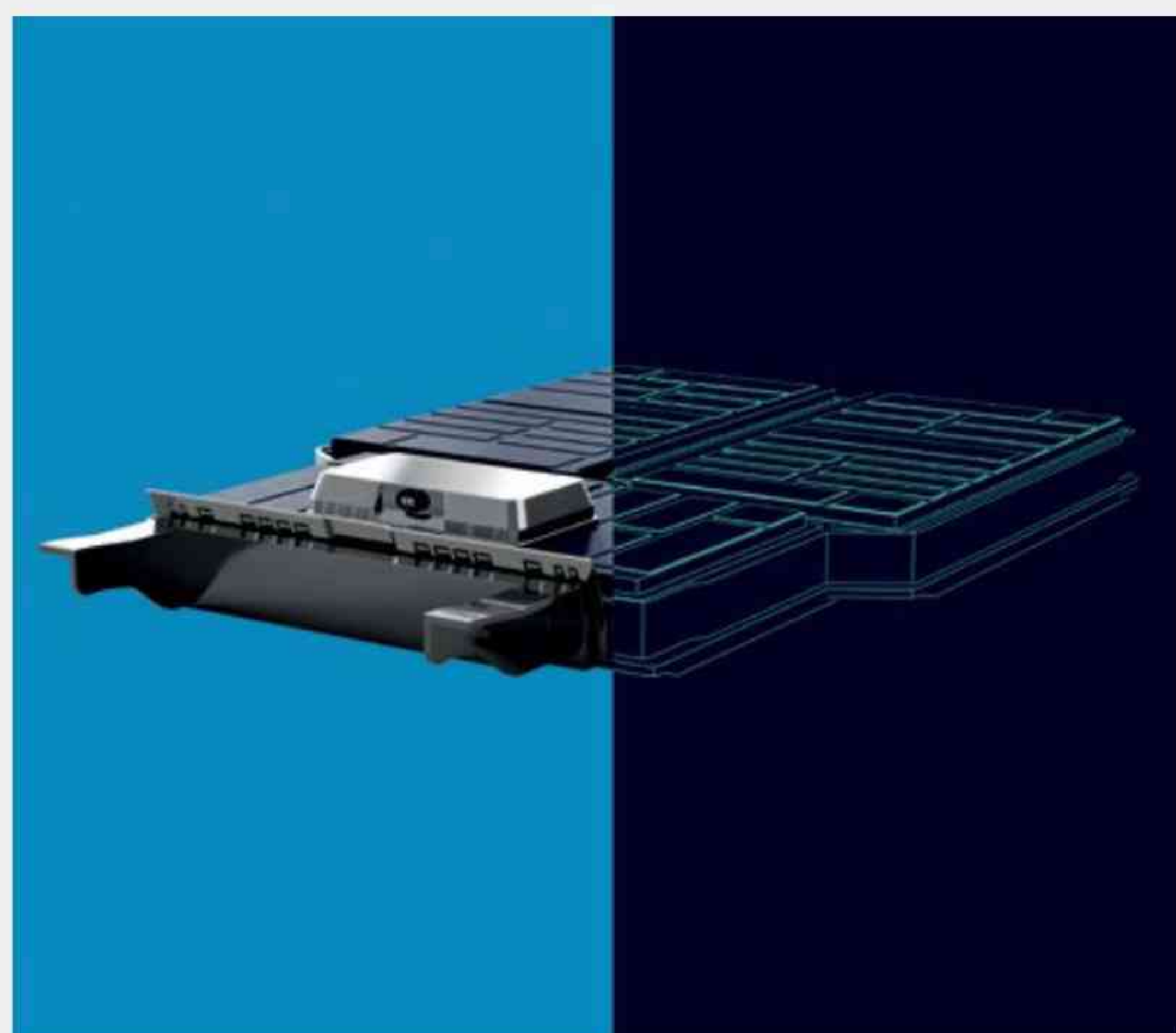
fiable de los nuevos buques. También prestará apoyo de diseño e ingeniería, colaborando estrechamente con WSF para garantizar la integración de la tecnología eléctrica híbrida en los nuevos barcos. Este enfoque de colaboración subraya el compromiso de

ABB de ofrecer soluciones a medida que satisfagan las necesidades específicas de sus socios.

“Es un honor que Washington State Ferries nos haya elegido como proveedor único de propulsión para los nuevos ferris híbridos eléctricos con capacidad para 160 automóviles”, ha señalado Drew Orvieto, vicepresidente de ventas de Marine Systems, US at ABB Marine & Ports. “Esta asociación pone de relieve nuestra visión compartida de la sostenibilidad y nuestra dedicación a ser pioneros en tecnologías avanzadas que impulsen el avance de la industria. Estamos deseando apoyar a WSF en su misión de ofrecer servicios de ferris más limpios y eficientes a las comunidades a las que sirven”.

Ael

SIEMENS SE INCORPORA A LA GLOBAL BATTERY ALLIANCE



■ La compañía promueve soluciones energéticas sostenibles.

Siemens Digital Industries Software se ha integrado en la plataforma colaborativa Global Battery Alliance (GBA) que reúne a las principales organizaciones internacionales, ONG, actores de la industria, academias y distintos gobiernos para alinearse colectivamente en un enfoque precompetitivo e impulsar el desarrollo en toda la cadena de valor de fabricación de baterías.

“Unirse a la Global Battery Alliance es un paso crítico que Siemens está dando para construir nuestro ecosistema de pasaporte de baterías, que tiene como objetivo ir más allá del cumplimiento normativo y capacitar a las partes interesadas para capturar, acceder y gestionar los datos de la cadena de valor de las baterías”, ha señalado Puneet Sinha, director senior de Battery Industry, Siemens Digital Industries Software. “Junto con la Global Battery Alliance y su comunidad, estamos ayudando a llevar el poder de la transformación digital a una industria de baterías de cara al futuro que sea eficiente, ética y sostenible”.

La visión de la plataforma es lograr tres resultados fundamentales, que la compañía respalda y a los que contribuye activamente: establecer una cadena de valor de baterías circular, establecer una economía baja en carbono a lo largo de la cadena de valor y salvaguardar los derechos humanos y el desarrollo económico. A través de la dedicación a estos principios, la compañía pretende lograr prácticas innovadoras y sostenibles para la industria de las baterías que no solo minimicen el impacto medioambiental, sino que también creen nuevas oportunidades de empleo y generen valor económico adicional para las comunidades de todo el mundo.

Ael



Antoni Rovira

Manager de Software y Control en Rockwell Automation Iberia



Fabricación inteligente 2024 en España

Hace unas semanas Sapio Research publicó un estudio titulado 'Estado de la fabricación inteligente 2024 en España', basado en encuestas realizadas a 70 empresas de fabricación nacionales. En el documento expone las oportunidades y los retos más importantes de la aplicación de las nuevas tecnologías en la industria local. Estos son algunos temas destacados:

- **Ciberseguridad a través de AI/ML:** El 87% de las empresas españolas afirmaron que ya han invertido, o tenían previsto invertir en los próximos meses, en Inteligencia Artificial (IA) y *Machine Learning* (ML) para soluciones ciberseguridad. Esta cifra es algo superior a la media europea (84%).

EL 87% DE LAS EMPRESAS ESTAN INVIRTIENDO EN IA Y ML PARA SOLUCIONES DE CIBERSEGURIDAD

- **Automatización, IA/ML:** Mientras que en Europa la mayoría de las empresas están pensando en dedicar más recursos a la automatización como prioridad principal, en España esta opción pasa a la tercera posición con un 37% de las empresas. Y en cambio, aquí hay preferencia por aumentar la externalización de trabajos, con un 47% de las respuestas (frente al 32% europeo), y a la introducción de IA/ML, con un 43% (33% en Europa).

- **Mejora de los procesos:** La aplicación de las nuevas tecnologías se orientará a incrementar la calidad según el 43% de las respuestas españolas, índice 2 puntos por encima de la media europea. Las siguientes prioridades son: el control de costes (42%), el crecimiento en nuevos mercados (33%) y la mejora en la sostenibilidad (33%).

- **Adopción de la tecnología:** Se considera un reto importante la incorporación de las nuevas tecnologías para mitigar riesgos, con un 28% de las respuestas.

- **Talento disponible:** La incorporación de nuevas tecnologías y disponer de recursos para darles soporte van totalmente correlacionados. Seguramente esta es la explicación para que la encuesta refleje la falta de personal cualificado como una preocupación importante para el 26% de las empresas españolas. En Europa este valor aumenta hasta el 31%.

LA FALTA DE PERSONAL CUALIFICADO ES UNA PREOCUPACIÓN IMPORTANTE PARA EL 26% DE LAS EMPRESAS

- **Sostenibilidad:** Las empresas españolas en cuestiones de ESG (*Environmental, Social and Governance*) se decantan por priorizar la mejora de la eficiencia (42%), seguido del cumplimiento de las normativas gubernamentales (34%) y la búsqueda de diferenciadores para ser más competitivos (33%). Las mayores preocupaciones pasan por aumentar la calidad y seguridad de los productos (39%), y seguidamente la reducción de residuos, reciclaje y gestión energética (36%).

En definitiva, los retos de la industria española en el momento de implementar proyectos de transformación digital están muy alineados con los de nuestros vecinos europeos. El estudio destaca una importante orientación hacia las nuevas tecnologías como IA/ML, con el objetivo de poder mejorar la ciberseguridad de los procesos, incrementar la calidad del producto, contener los costes, mejorar la sostenibilidad, y a la vez que conseguir el crecimiento en nuevos mercados. Pero, considera un reto incorporar estas nuevas técnicas, y buena parte de ello está asociado a la falta de personal cualificado para llevar a cabo los procesos de cambio necesarios.

Por tanto, la atracción de talento, su formación continua, y retención del personal cualificado se convierten en estrategias clave, con incidencia notable en el futuro de muchas empresas. ●



Aumenta la visibilidad de tu empresa de industria 4.0

Únete a la asociación líder de la robótica y automatización en España:

1. Networking con entidades de todo tipo (multinacionales, empresas emergentes, centros tecnológicos, etc.), a través de iniciativas como los Grupos de Trabajo y las Comisiones AER, de tu asistencia a nuestro SUMMIT y de tu participación en los stands conjuntos y otras actividades que organizamos durante las ferias sectoriales más importantes.

2. Visibilidad ante las Administraciones públicas y CEOE-CEPYME, y también mediante nuestros canales de comunicación, como el anuario INSIGHT (tirada de 2.000 ejemplares), nuestro perfil en LinkedIn (+8.000 seguidores), nuestra newsletter mensual (+800 profesionales del sector) y nuestra revista digital Automation REVIEW. Las mesas redondas y los tours tecnológicos que organizamos durante los eventos sectoriales te aportarán también una gran proyección.

3. Información sobre ayudas públicas para I+D e internacionalización, además de datos en primicia sobre el mercado gracias a nuestros estudios internos y a las colaboraciones con instituciones como IFR, de la que somos miembros fundadores y representantes oficiales en España, VDMA, A3, amec y Odense Robotics.



aer-automation.com

¡HAZTE SOCIO!

Avances, aplicaciones, retos y perspectivas

VISIÓN ARTIFICIAL

La visión artificial ha evolucionado de manera extraordinaria gracias al *Deep Learning*, revolucionando sectores como la robótica, la automatización y el control de calidad. Las aplicaciones van desde la manipulación de objetos complejos hasta la agricultura y el reciclaje, transformando procesos tradicionales y aumentando la eficiencia en diversos entornos industriales.

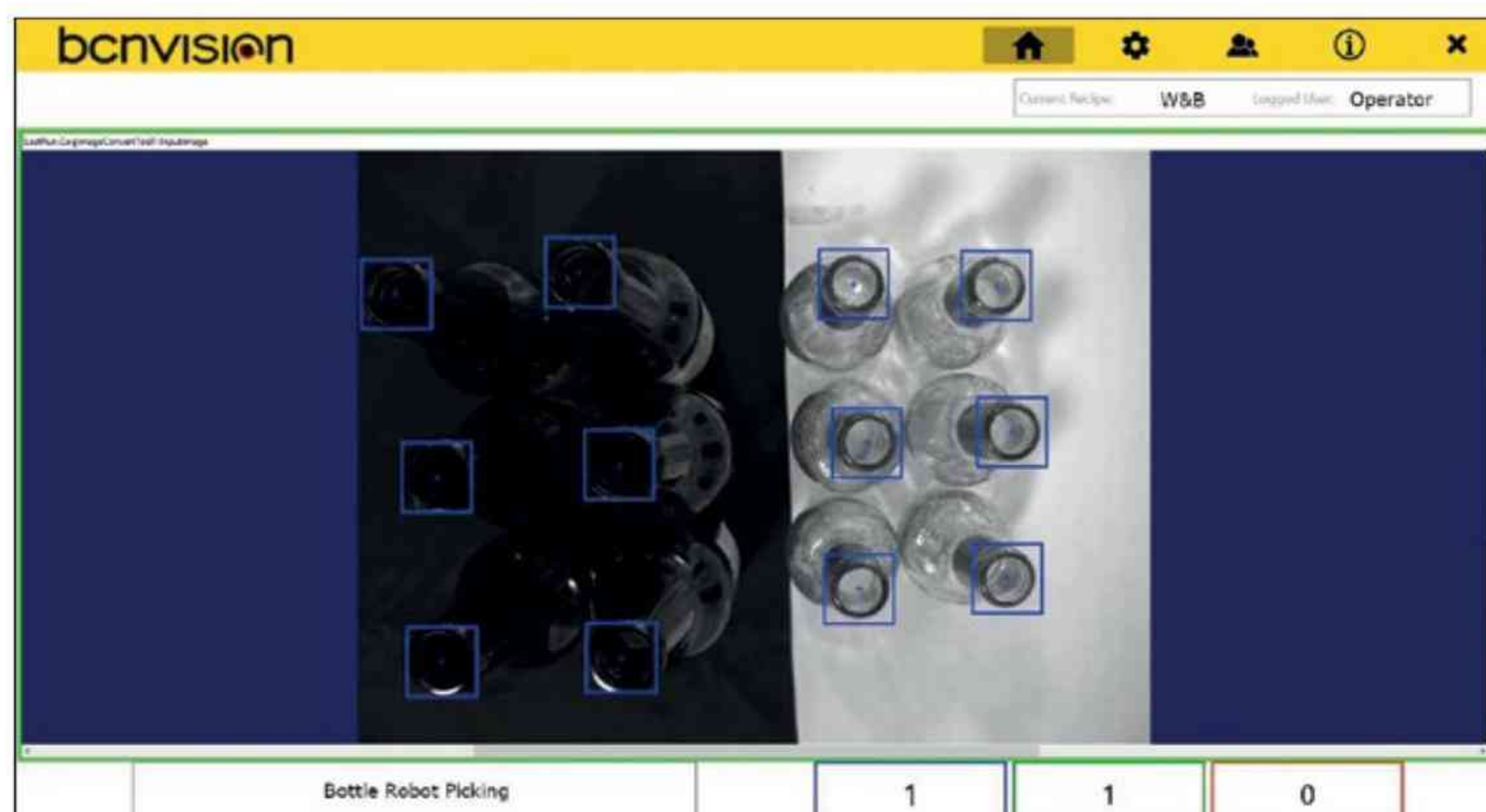
■ **Grupo de Trabajo de Innovación de la Asociación Española de Robótica y Automatización (AER Automation)** 

La visión artificial ha recorrido un largo camino desde sus inicios, pasando de ser una tecnología complementaria a convertirse en una herramienta clave en la automatización industrial moderna. Impulsada por avances en el *Deep Learning*, ha permitido un nivel de precisión y adaptabilidad que sería impensable con métodos tradicionales. En este artículo exploraremos los aspectos más destacados de la visión artificial aplicada a la automatización y cómo esta tecnología está configurando el futuro de la industria.

Avances y aplicaciones en visión industrial

Uno de los mayores retos en la automatización ha sido la falta de flexibilidad en entornos cambiantes. Durante años, la robótica ha dependido de sistemas deterministas, diseñados para realizar tareas repetitivas en condiciones controladas. Sin embargo, la introducción de la robótica guiada por visión ha cambiado este panorama, permitiendo que los robots adapten sus acciones en función del entorno que perciben en tiempo real.

Ejemplos como el control de calidad en líneas de producción muestran cómo la visión artificial ayuda a detectar defectos a medida que las piezas avanzan en una cinta transportadora. Herramientas como el AI Error Proofing permiten clasificar automáticamente las piezas, mejorando la eficiencia y reduciendo costes. En aplicaciones más avanzadas, los sensores 3D y las redes neuronales

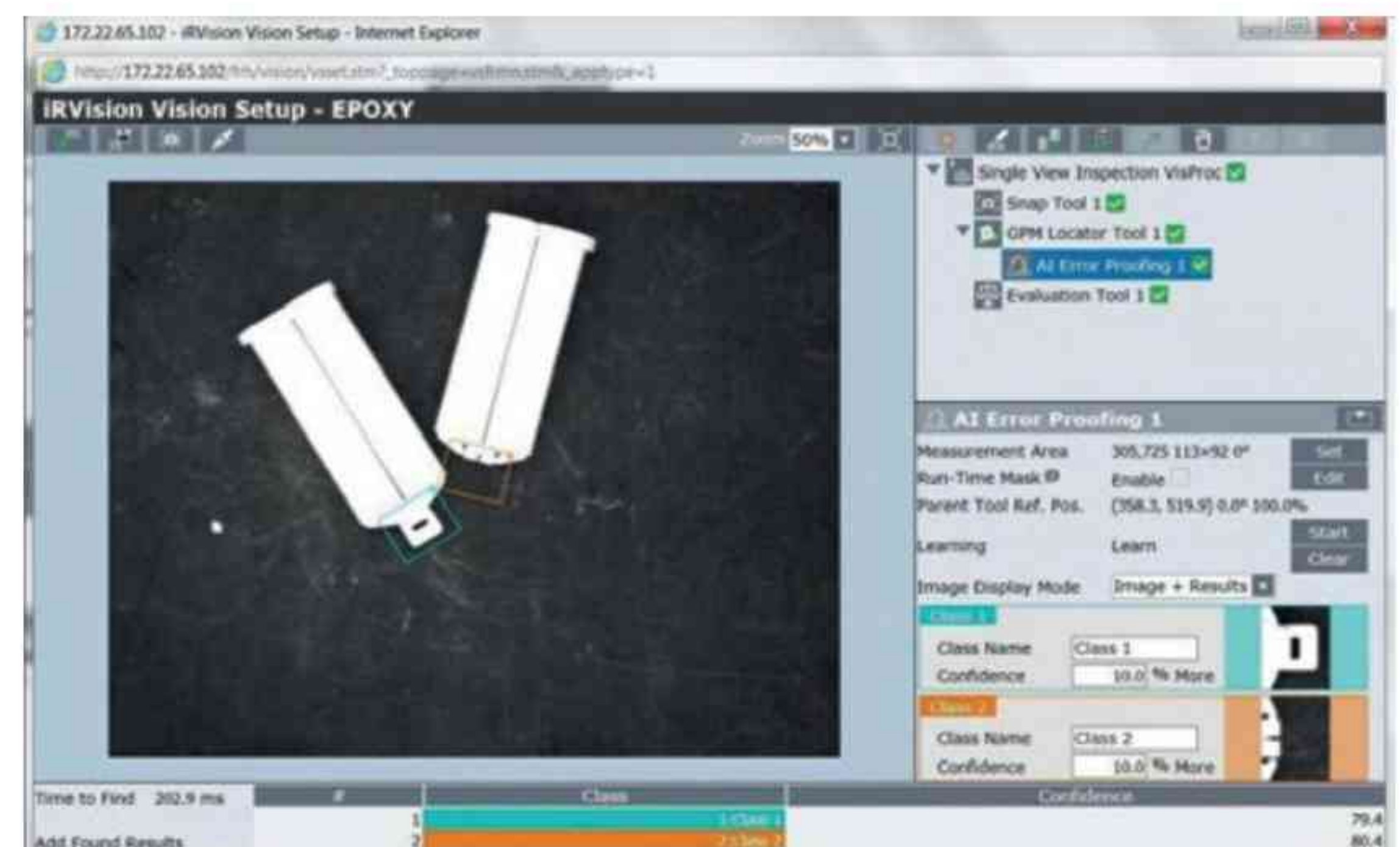


La solución de visión artificial basada en *Deep Learning* desarrollada por bcvision, permite entregar la posición a un robot de cualquier tipo de botella de cristal de una forma rápida, eficiente y precisa.

detectan objetos sin necesidad de modelos CAD, lo que facilita la manipulación de piezas irregulares o naturales, como se vio en el proyecto SpecTUNA, donde se automatizó la detección y el procesamiento de atunes para su corte y clasificación.

El *Deep Learning* ha jugado un papel crucial en la transformación de la visión artificial. Técnicas como la detección de anomalías y la segmentación semántica permiten clasificar píxeles en una imagen o detectar errores sin necesidad de contar con grandes cantidades de datos defectuosos. Por ejemplo, en el control de calidad de botellas de vidrio, donde la variabilidad del material y los reflejos dificultan el proceso, las redes neuronales han permitido superar estos desafíos al iden-

tificar correctamente los cuellos de las botellas, a pesar de la baja repetitividad y el contraste de las imágenes. La combinación de redes neuronales convolucionales (CNN) y arquitecturas más avanzadas, como las basadas en *Transformers*, ha permitido resolver problemas complejos en tiempo real, como la clasificación de materiales en la industria del reciclaje o la detección de plagas en la agricultura. En este último campo, el proyecto Greenpatrol ha desarrollado un robot que, mediante técnicas de *Deep Learning*, inspecciona plantas en invernaderos para detectar plagas en distintas fases de su ciclo de vida y aplicar insecticidas de forma precisa, reduciendo el uso innecesario de químicos y mejorando la sostenibilidad de la producción agrícola.



La nueva herramienta AI Error Proofing iRVision de FANUC facilita la adición de pruebas de errores a cualquier aplicación de robot FANUC.

Herramientas y recursos accesibles

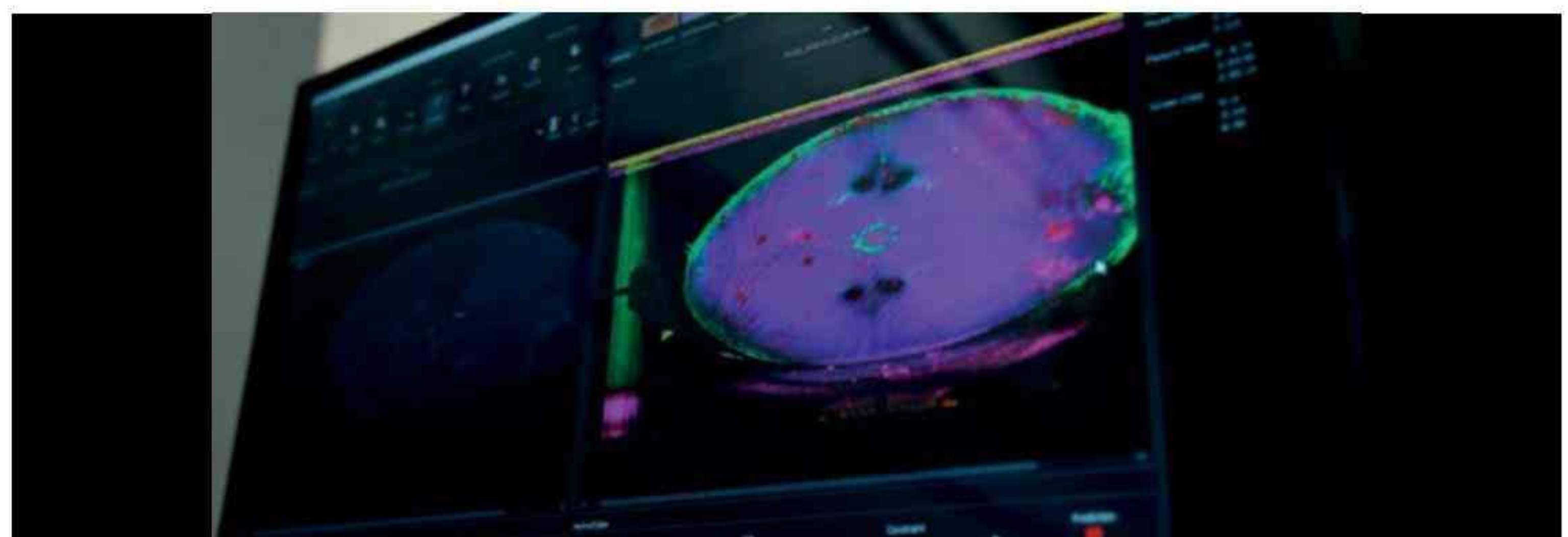
Gracias al desarrollo de frameworks de *Deep Learning* como TensorFlow y PyTorch, hoy en día es más fácil que nunca implementar redes neuronales en proyectos de visión artificial. Estas herramientas, junto con la disponibilidad de grandes bases de datos públicas como Imagenet o MS-COCO, permiten a los desarrolladores entrenar modelos con una eficiencia antes impensable. Además, los repositorios de código abierto, como GitHub, y los hubs de modelos preentrenados han facilitado el acceso a soluciones avanzadas, reduciendo el tiempo y coste de desarrollo.

La posibilidad de utilizar modelos preentrenados en diferentes tareas ha abierto un nuevo abanico de oportunidades, desde la segmentación de imágenes hasta la detección de objetos. Los desarrolladores pueden aprovechar estos recursos para adaptar las redes neuronales a sus necesidades específicas, lo que ha acelerado la adopción de la inteligencia artificial en múltiples industrias.

Retos futuros y perspectivas

A pesar de los avances, la visión artificial aún enfrenta varios desafíos. El entrenamiento de modelos de *Deep Learning* requiere grandes cantidades de datos y recursos computacionales significativos, lo que puede ser una barrera para pequeñas empresas. Además, la introducción de nuevas arquitecturas, como los *Transformers*, aumenta la demanda de hardware, lo que limita quién puede llevar a cabo estos desarrollos.

Otro reto clave es evitar sesgos en los datos utilizados para entrenar las redes neuronales. Si los conjuntos de datos no son representativos de la realidad, los modelos pueden generar resultados inexactos o incluso discriminatorios. Esto



El proyecto europeo SpectUNA, en el que participa Stemmer Imaging, consiste en un sistema modular automatizado con visión artificial y escaneo láser 3D para los procesos de posicionamiento, corte y clasificación de atún congelado.

subraya la importancia de una curación cuidadosa de los datos, así como de la diversidad en los mismos. Por otro lado, el análisis de datos en vídeo y la integración del 5G abrirán nuevas oportunidades en la visión artificial. Tecnologías como la computación en la nube permitirán procesar grandes cantidades de datos en tiempo real, eliminando la necesidad de costosos equipos locales y facilitando el acceso a soluciones avanzadas de visión para empresas de todos los tamaños.

La visión artificial, potenciada por el *Deep Learning*, está transformando la industria moderna, permitiendo niveles de automatización y precisión nunca antes vistos. Desde el control de calidad hasta la agricultura de precisión, las aplicacio-

nes de esta tecnología son tan diversas como sus beneficios. Sin embargo, aún hay retos por superar, desde el acceso a hardware adecuado hasta la curación de datos. Lo que está claro es que el futuro de la visión artificial es brillante, y su evolución seguirá impactando profundamente en la eficiencia y sostenibilidad de los procesos industriales. ●

Acceda al artículo completo



JENNIFER PRGESA

Senior Product Manager en Honeywell Connected Enterprise

36

Los simuladores son el mejor sustituto para operaciones reales en un entorno seguro”

Los sistemas de entrenamiento de operadores (OTS) han evolucionado hasta convertirse en gemelos digitales, transformando la forma en que la industria aborda la formación y optimización de procesos. Con tecnologías como la computación en la nube y simuladores dinámicos de alta fidelidad, es posible ofrecer soluciones que mejoran la eficiencia, la seguridad y el retorno de inversión, permitiendo un entrenamiento realista en un entorno seguro. Charlamos con Jennifer Prgesa, Senior Product Manager en Honeywell Connected Enterprise, para descubrir el impacto y futuro de estos sistemas.

Automática e Instrumentación

“Hemos tenido clientes que han reportado hasta 6 veces el retorno de su inversión con el simulador de entrenamiento de Honeywell”, destaca Jennifer Prgesa durante la entrevista.

Automática e Instrumentación: Los denominados sistemas para el entrenamiento de operadores (OTS) existen en la industria desde hace varias décadas. ¿Cómo han evolucionado hasta convertirse en verdaderos ‘gemelos digitales’ y cuáles han sido los avances tecnológicos que han facilitado esta conversión?

Jennifer Prgesa: Los sistemas de formación de operadores representan una colección de gemelos digitales que sirven para muchos casos de uso. El modelado de procesos, la evolución de los controladores y la potencia de computación son solo algunos de los avances tecnológicos clave que han llevado a los simuladores dinámicos de formación a convertirse en verdaderos gemelos digitales. Los modelos subyacentes se han convertido en representaciones más precisas de la dinámica del proceso y del sistema de control, mientras que la implementación de los datos se ha hecho más flexible a medida que mejoraba la tecnología.

Ahora, los modelos de procesos – cuando se aprovechan en otro software con conectividad a datos en tiempo real y capacidades de limpieza de datos, u otras capacidades clave necesarias – pueden utilizarse para el análisis de escenarios, la detección y la optimización de procesos, además de la instrucción de la mano de obra. Los modelos más precisos suelen requerir mayores recursos informáticos para simular los cambios a tiempo real. Por lo tanto, la mejora de la potencia de cálculo es también un factor importante. Recientemente, Honeywell también ha aprovechado las tecnologías en la nube para beneficiarse de los avances computacionales y arquitectónicos, así como para permitir la colaboración en cualquier momento y lugar.

Ael: ¿Cómo se utilizan estos sistemas para la mejora de la eficiencia y seguridad de los sistemas de control?

J.P.: Los simuladores dinámicos de formación de Honeywell, además de la instrucción experimental, pueden verificar bases de datos de sistemas de control y seguridad, lo que permite a los clientes realizar pruebas antes de su implementación en un sistema de producción. Los clientes también pueden realizar análisis de ingeniería desarrollando, probando y optimizando procedimientos y cambios en el diseño de procesos. Todo ello puede ayudar a proporcionar a los clientes ahorros de tiempo, medidas de seguridad adicionales e incluso una producción optimizada, mejorando la eficiencia de sus operaciones.

Ael: ¿Qué papel juegan los sistemas OTS en la formación y certificación de nuevos operadores?

J.P.: Nuestros clientes consideran que los simuladores dinámicos de formación son uno de los medios más importantes para certificar a los nuevos operadores. Un simulador de aprendizaje de alta fidelidad puede simular procedimientos operativos importantes, así como proporcionar informes detallados sobre la capacidad de los operadores para manejar los escenarios basándose en métricas personalizables. Los simuladores de formación son el mejor sustituto cuando se trata de practicar y experimentar operaciones muy cercanas a la realidad en un entorno seguro, con la ventaja añadida de generar evaluaciones para el establecimiento de bases requeridas y el seguimiento de las competencias.

Ael: ¿Cómo se mide el retorno de la inversión (ROI) de un sistema de este tipo y qué factores pueden afectar a este ROI?

J.P.: El ROI se mide generalmente en dólares gastados y ahorrados/ganados por la compra de activos de simulador. Los beneficios de un simulador de formación pueden presentarse de muchas formas, como una recuperación más rápida de las alteraciones del proceso, transiciones de grado (condiciones de funcionamiento) más rápidas, arranques y paradas más suaves, mayor disponibilidad de la instrucción y la reducción de sus costes. Hemos tenido clientes que han reportado hasta 6 veces el retorno de su inversión con el simulador de entrenamiento de Honeywell.

Ael: ¿Qué diferencia la propuesta de Honeywell de otras propuestas del mercado?

J.P.: Los simuladores de formación de Honeywell se diferencian en la tecnología subyacente, las medidas de protección de la propiedad intelectual y la experiencia del equipo de entrega. Desde el punto de vista tecnológico, Honeywell utiliza su propio y robusto motor dinámico de procesos para crear soluciones de instrucción estables y de alta fidelidad que se integran de forma nativa reduciendo o eliminando la necesidad de modificaciones manuales.

La cartera tecnológica de Honeywell también incluye herramientas de fácil integración con el DCS del cliente y soluciones adicionales de gestión de competencias a nivel empresarial. Las soluciones de Honeywell están diseñadas para proporcionar un alto nivel de seguridad para controlar el acceso a cualquier IP propiedad de los clientes. Las funciones de evaluación de Honeywell, líderes en el sector, que pueden alimentar directamente las herramientas de mapeo de competencias, permiten establecer una base y realizar un seguimiento de las competencias.

Por último, la organización de entrega de Honeywell tiene un historial probado de entrega de simuladores de formación que se adapta a las necesidades de cada uno de sus clientes a lo largo de los años. Gracias a su competente y experimentado equipo de entrega, Honeywell puede personalizar los simuladores de formación para adaptarlos a las necesidades de cada cliente y colaborar con ellos para comprender sus objetivos e incluso crear modelos con ellos. Más allá de la tecnología, vemos los simuladores dinámicos de formación como una herramienta más amplia para la educación. Las soluciones de aprendizaje de Honeywell están diseñadas para acompañar a las empresas en la evolución de su plantilla, permitiéndoles no solo formar eficazmente, sino también planificar programas de instrucción para toda la empresa y crear nuevas oportunidades para su personal. ●

Propuesta innovadora que destaca por su seguridad, eficacia y practicidad

LOS DELTA D-BOTS GANAN EL 'RED DOT: BEST OF THE BEST' 2024 POR SU DISEÑO Y CREATIVIDAD DE VANGUARDIA

Los robots colaborativos están revolucionando varios sectores industriales al aumentar la eficiencia y la productividad. Diseñados para trabajar junto a los humanos, combinan a la perfección el trabajo manual con la automatización avanzada, desbloqueando nuevos niveles de innovación y resultando indispensables para un lugar de trabajo colaborativo y vanguardista. En la amplia variedad de robots colaborativos son los D-Bots, los cobots de Delta Electronics, los que destacan y han ganado el prestigioso premio 'Red Dot: best of the best' 2024, con un diseño innovador que hace hincapié en la seguridad, la eficiencia y la practicidad.



Los seis modelos presentan cargas útiles de entre 6 kg y 30 kg, varios tamaños, alcances de 800mm a 1.800 mm y una precisión de $\pm 0,02$ mm.

La gama D-Bot de Delta Electronics está diseñada para integrar a la perfección la automatización avanzada en las operaciones cotidianas de las más distintas industrias. Presentada en la Hannover 2024, ha suscitado un gran interés desde el primer momento. Los seis modelos presentan cargas útiles de entre 6 kg y 30 kg, varios tamaños, alcances de 800mm a 1.800 mm y una precisión de $\pm 0,02$ mm. Alcanzan velocidades de hasta 200 grados por segundo y una flexibilidad y precisión inigualables gracias a los 6 ejes. Cada D-bot destaca por su facilidad de uso, sus sólidas funciones de seguridad y su versatilidad, características que le han permitido ganar el coticiado premio del Red Dot Design Award.

Intuitivo y versátil

Los cobots Delta han sido diseñados para una instalación rápida y un uso sencillo, ofreciendo funcionalidad *plug-and-play* y una configuración intuitiva. La programación es muy visual y user friendly y se pueden instalar en menos de tres horas. No se requieren conocimientos especializados, es suficiente un pequeño periodo de formación para capacitar al personal de la empresa en el uso de los D-Bots.

Aptos para una amplia variedad de aplicaciones como paletizado, *pick & place*, soldadura, envasado y muchas más, son el aliado ideal para numerosas industrias. La versatilidad de los D-Bots también se manifiesta en las distintas posibilidades de montaje. De hecho, pueden instalarse en cual-

quier orientación: vertical, horizontal o incluso desde arriba hacia abajo. Esta flexibilidad maximiza la eficiencia del espacio y se adapta a una gran variedad de disposiciones operativas.

Seguridad como prioridad absoluta

Como los cobots están ideados para interactuar con personas en entornos de producción, la seguridad desempeña un papel muy importante en el diseño del producto. La innovadora función de seguridad 'Reflex Safety' reconoce el contacto a la velocidad del rayo e invierte el movimiento inmediatamente para evitar accidentes y proteger tanto al personal como al equipamiento. Además, la integración de sensores de alta gama y la detección de colisiones ('one-finger tap') maximizan la seguridad.

En la mayoría de los cobots, los brazos están diseñados para detenerse inmediatamente al entrar en contacto con una persona, para evitar golpearla. Pero la interrupción puede no ser suficiente, ya que podría, por ejemplo, inmovilizar a un trabajador en una posición antinatural o peligrosa. Los D-Bots no sólo se detienen al entrar en contacto con la persona, sino que invierten el movimiento, algo parecido a lo que ocurre cuando tocamos una superficie caliente y, por reflejo, retraemos la mano inmediatamente.

Esta perfecta integración de la seguridad permite una estrecha colaboración humano-robot sin barreras, transformando los D-Bots de simples herramientas a miembros esenciales del equipo.

Precisión y fiabilidad

Cada D-Bot ofrece una precisión inigualable en diversas aplicaciones, garantizando un rendimiento y una fiabilidad constantes.



■ La integración de sensores de alta gama y la detección de colisiones ('one-finger tap') maximizan la seguridad.

■

**LOS COBOTS DELTA
HAN SIDO DISEÑADOS
PARA UNA INSTALACIÓN
RÁPIDA Y UN USO
SENCILLO, OFRECIENDO
FUNCIONALIDAD
PLUG-AND-PLAY Y
UNA CONFIGURACIÓN
INTUITIVA**

La integración de encoders 24 bits permite alcanzar la máxima resolución y aumentar aún más la precisión. El margen de repetibilidad es de $\pm 0,02$ mm, comparable al de los robots industriales. Además de una precisión absoluta, el D-Bot ha sido diseñado para garantizar la eficacia y la seguridad en los entornos más hostiles. De hecho, su estructura es compacta y duradera, y ha sido equipado con protección IP66 y protocolos de seguridad avanzados. Por tanto, la serie D-Bot de Delta promete un espacio de trabajo seguro y eficiente, generando el entorno perfecto para la colaboración hombre-máquina.



■ José Pedro Gutiérrez Salgado,
Country Manager
IABG Delta
Electronics Iberia.

Delta Electronics
www.deltaww.com



SEMICON
EUROPA



November 12–15, 2024
**Leading the
way to the
future of AI**

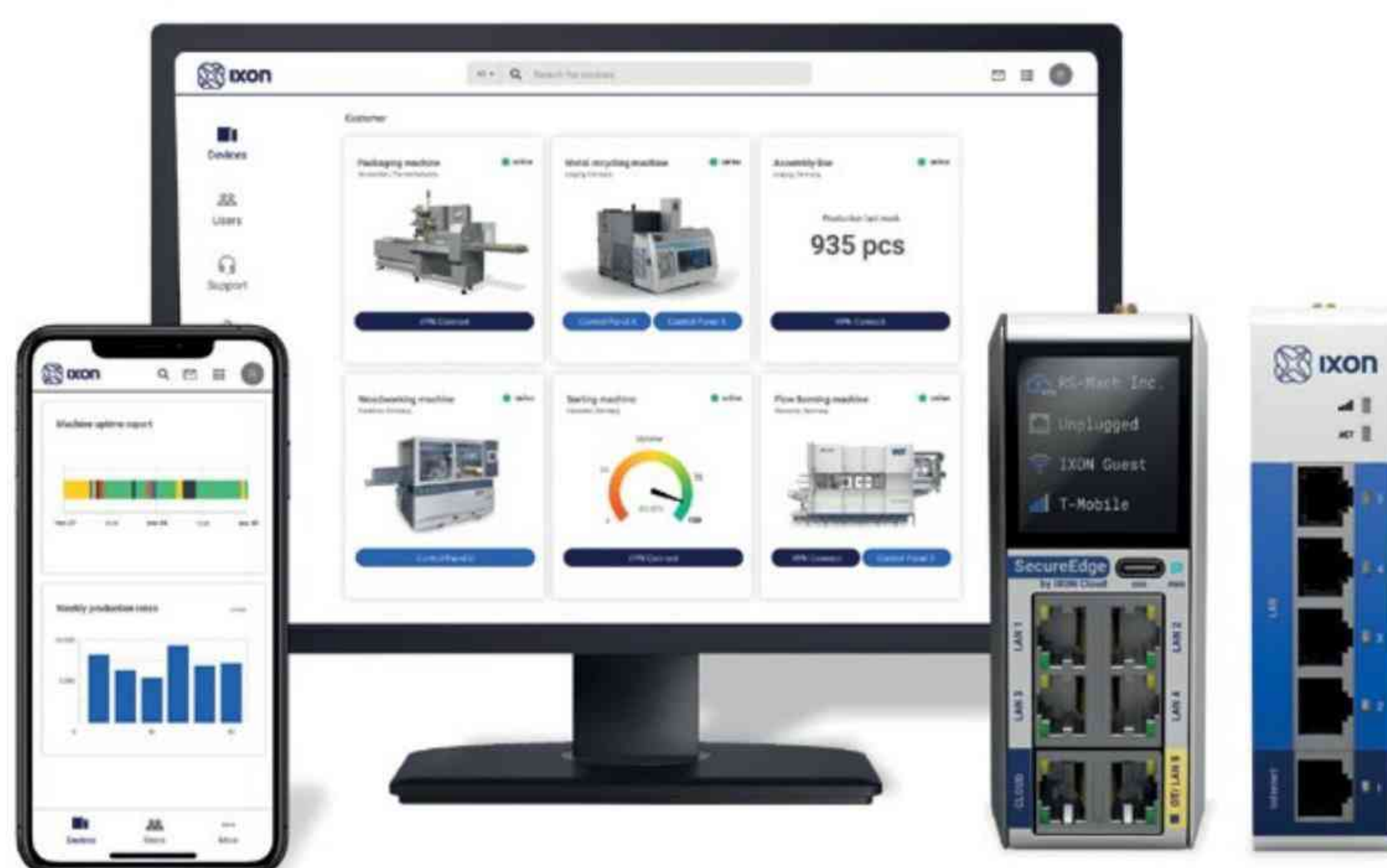
powered by electronica
World's leading trade fair and conference for electronics

Get your ticket now!
electronica.de/tickets

De la mano de RTC, las claves para el futuro del servicio en la fabricación

IXON COMO PLATAFORMA IIOT PARA FABRICANTES DE MAQUINARIA

La solución integral de IXON ayuda a los fabricantes de maquinaria a prestar un mejor servicio a sus clientes, proporcionando a través de su plataforma acceso remoto seguro y servicios adicionales relacionados con la Industria 4.0. Como *partner* de IXON, RTC cuenta con un equipo técnico experto dispuesto a ayudar a los fabricantes de maquinaria a optimizar su eficiencia operativa y a avanzar en su transformación digital; acompañándole desde la idea hasta la implementación de su proyecto.



RTC
Regulació Tècnica i Control



IXON ofrece una solución de IIoT integral para todas las necesidades de mantenimiento y servicios remotos: desde el hardware hasta la nube.

RTC – Regulació, Tècnica i Control, con más de 30 años en el sector de la automatización; busca ofrecer las mejores soluciones para el mundo de la automatización industrial, tecnología eléctrica y comunicaciones. Para ello, trabaja de la mano con IXON para brindar productos y servicios para la digitalización de maquinarias y plantas de producción.

Una solución IIoT integral

IXON y RTC comparten la visión de que el fabricante de máquinas del futuro es un proveedor de servicios y todas sus estrategias deben enfocarse en ello. La estrecha colaboración entre los fabricantes y los propietarios de máquinas añadirá valor al servicio, reducirá los costes y el tiempo de inactividad de las máquinas, redundando en un beneficio para ambas partes.

Para todo ello, IXON ofrece una solución de IIoT integral para todas las necesidades de mantenimiento y servicios remotos: desde el hardware hasta la nube.

IXON Y RTC IMPULSAN LA TRANSFORMACIÓN DIGITAL DE LOS FABRICANTES DE MAQUINARIA CON SOLUCIONES DE IIOT, CONECTIVIDAD SEGURA Y SERVICIOS ENFOCADOS EN LA EFICIENCIA OPERATIVA

IXrouter: conectividad segura y eficiente

IXON ofrece todos sus servicios mediante un router industrial VPN, el IXrouter. Este dispositivo se conecta a su LAN industrial mediante Ethernet y se conecta a su WAN mediante Ethernet, WiFi o 4G, conectando su PLC o HMI con el resto del mundo de forma segura. Características destacadas:

- Switch integrado.
- Servidor y cliente DHCP simultáneo.
- Servidor NTP.
- WiFi Hotspot.
- Firewall integrado fácil de configurar.
- Sistema no intrusivo a tu red de automatización.

Acceso remoto simplificado con IXON Cloud

La conexión a acceso remoto se realiza través del portal de IXON Cloud cuyo funcionamiento es sencillo, incluso para quienes no son expertos en tecnología. Con un solo clic en IXON Cloud, o desde la aplicación de IXON para smartphones (tanto iOS como Android), se puede acceder a todos los servicios de IXON, solo se requiere una conexión a internet. Algunas de las características del portal de IXON son:

- Posibilidad de establecer túneles VPN ilimitados y simultáneos.
- Acceso a los servidores WEB y VNC de los equipos sin necesidad de establecer un VPN.
- Configuración de los equipos.
- Gestión de usuarios.
- Gestión de alarmas.
- Visualización de datos en tiempo real e históricos.
- Sistema compatible con la gran mayoría de sistemas de automatización industrial.

IXROUTER

GARANTIZA UN ACCESO SEGURO A TRAVÉS DE MÚLTIPLES OPCIONES COMO ETHERNET, WIFI Y 4G, ASEGURANDO UNA INTEGRACIÓN SIN INTERRUPCIONES EN REDES DE AUTOMATIZACIÓN

Preparados para los desafíos del futuro

Además del IXrouter3, IXON ha desarrollado el SecureEdge Pro, un nuevo router que implementa tecnología Docker para desarrollar sistemas de Edge Computing desde un entorno amigable.

El compromiso de IXON con la ciberseguridad permite evitar incidencias de seguridad:

- Red mundial de servidores redundantes.
- Datos almacenados dentro de la EU.
- Certificaciones ISO-9001 e ISO-27001 / ISO-27017/ ISO-27701
- Cumple con los requisitos de IEC 62443-4-1 y 4-2.
- Preparados para cumplir con la NIS2.

RTC e IXON ayudan a los fabricantes de maquinaria hacia su transformación digital con una solución enfocada en dar servicio a los clientes. Más de 2500 fabricantes de maquinaria de todo el mundo, ya confían en IXON. Los nuevos desafíos creados por la digitalización del mundo industrial pueden ser resueltos con la ayuda de IXON y RTC

RTC - Regulació, Tècnica i Control

www.rtcautomatismos.com

rtc@grupcarol.com

(+34) 93 570 2644

coneQtia

Asociación de Prensa Profesional
y Contenidos Multimedia

Conectamos conocimiento desde 1925

Información para decidir

Solo aquella información basada en la responsabilidad y la calidad **nos hace libres para tomar las mejores decisiones profesionales**. En ConeQtia, entidad colaboradora de CEDRO, garantizamos contenido riguroso y de calidad, elaborado por autores especializados en más de 30 sectores profesionales, con el aval de nuestros editores asociados y respaldando el uso legal de contenidos. Todo ello con la finalidad de que **el lector pueda adquirir criterio propio, facilitar la inspiración en su labor profesional y tomar decisiones basadas en el rigor**.

Por este motivo, todos los editores asociados cuentan con el **sello de calidad ConeQtia**, que garantiza su profesionalidad, veracidad, responsabilidad y fiabilidad.

Con la colaboración de:



coneqtia.com

La revolución digital llega a la planificación urbana

IA Y CIUDAD: EL AMANE CER DE UNA NUEVA ERA EN EL URBANISMO

Estamos al borde de una revolución tecnológica sin precedentes, donde la inteligencia artificial (IA) emerge no solo como una herramienta más, sino como el catalizador que podría redefinir la humanidad misma. Al igual que el fuego, la rueda o la electricidad, la IA representa un salto evolutivo en nuestra capacidad para transformar el mundo que nos rodea. En campos tan diversos como la medicina, la ingeniería y el urbanismo, su impacto comienza a sentirse, pero es solo el preludio de lo que está por venir. / Imágenes: EUROPEAN SCHOOL OF ARCHITECTURE

■ **Vicente Molina Domínguez**, Arquitecto e Ingeniero de la Edificación 



El progreso de la IA plantea nuevas preguntas y desafíos, pero, como en otras revoluciones tecnológicas, la adaptación será clave para su integración exitosa en la planificación urbana.

En el municipio de Villa Serena, un lugar enclavado entre montañas y valles verdes, la vida parecía discurrir sin grandes sobresaltos. Era un lugar donde el tiempo avanzaba a un ritmo propio, lejos del bullicio y las tendencias globales. Sin embargo, para Julián Herrera, el alcalde de aquel municipio, esa calma era solo una fachada. Cada día enfrentaba desafíos que los habitantes rara vez veían: una infraestructura anticuada, falta de inversión en transporte público, y problemas habitacionales que amenazaban con transformar la idílica vida rural en una carga insostenible. Como alcalde, se sentía constantemente abrumado, y la esperanza de poder cambiar las cosas se desvanecía con cada reunión con el ayuntamiento.

Julián había sido un ferviente defensor del progreso durante su campaña electoral, convencido de que el futuro de Villa Serena dependía de modernizarse. Pero dos años después de asumir el cargo, los proyec-

tos parecían más trabas que avances. Se sentaba en su despacho, en medio de informes sobre proyectos estancados y quejas de los ciudadanos, sintiendo el peso del cargo sobre sus hombros.

Una tarde, mientras revisaba correos electrónicos, uno llamó su atención. El remitente era desconocido: "AETHER: Urbanismo inteligente". Julián frunció el ceño, intrigado, y abrió el mensaje.

"Estimado alcalde Herrera, Le presentamos AETHER, una inteligencia artificial diseñada para transformar las ciudades mediante análisis avanzados de datos y optimización de recursos. AETHER ya ha sido implementada con éxito en ciudades como Singapur, Doha y San Francisco, logrando mejoras sustanciales en movilidad, planificación urbana y sostenibilidad. Estamos buscando ciudades emergentes que deseen mejorar su infraestructura con nuestra tecnología. Nuestra fase beta es completamente gratuita, y creemos que Villa Serena

podría beneficiarse enormemente de nuestra herramienta. Si está interesado, no dude en contactarnos."

Julián leyó el mensaje varias veces, desconfiando. Una IA que resolvía problemas urbanos. La sola idea de dejar que una máquina sugiriera cómo debía dirigir su municipio le parecía demasiado arriesgada. Sus compañeros en el ayuntamiento, especialmente los más veteranos, lo ridiculizarían solo por mencionarlo. Pero algo en aquel mensaje le hacía pensar que podría ser lo que necesitaba. Había oído hablar de Singapur y su eficiente infraestructura, de cómo San Francisco estaba liderando el camino en sostenibilidad. ¿Podría una IA realmente funcionar en un lugar como Villa Serena?

Esa misma tarde, en una reunión del ayuntamiento, Julián decidió mencionar la oferta de AETHER. Como había previsto, la reacción fue inmediata. —¿Una inteligencia artificial? —dijo Ernesto, el regidor de obras públicas, soltando una risa sarcástica—. ¿Y qué será lo siguiente? ¿Que una máquina nos diga cómo plantar patatas también?



La IA se presenta cómo un gran aliado para los retos que presenta el urbanismo del futuro.

—El problema, Julián —añadió Marta, la concejala de urbanismo, con tono serio—, es que estás buscando una solución fácil. Esto no es San Francisco, ni Singapur. Aquí tenemos nuestras particularidades.

—No estoy diciendo que debamos implementar nada de inmediato —respondió Julián, sintiendo cómo la reunión se le escapaba de las manos—. Solo sugiero que lo probemos. Es gratuito, y podría darnos ideas que no hemos considerado. No perdemos nada.

Pero la mayoría de los presentes ya había tomado su decisión. Para ellos, la tecnología de vanguardia no tenía cabida en un lugar como Villa Serena. Julián, sin embargo, no estaba dispuesto a rendirse tan fácilmente. Tras la reunión, con una mezcla de frustración y determinación, decidió ponerse en contacto con los responsables de AETHER.

Al día siguiente, recibió una respuesta rápida y clara: el software estaba listo para ser activado, y uno de los

“LA LLEGADA DE LA SINGULARIDAD O LA INTELIGENCIA ARTIFICIAL SUPERINTELIGENTE ES UN TEMA RECURRENTE EN LOS DEBATES CIENTÍFICOS, CON UNA POSIBLE APARICIÓN HACIA 2060”

ingenieros de AETHER se ofreció a guiarle en los primeros pasos. Con un poco de temor, pero también con esperanza, Julián aceptó.

El ingeniero, un hombre joven y apasionado llamado Marcos, le explicó que AETHER funcionaba mediante la recopilación de datos geoespaciales, históricos y demográficos, analizando patrones de tráfico, infraestructura y comportamiento ciudadano. Lo primero que debían hacer era cargar toda la información disponible sobre Villa Serena: mapas, censos, registros de transporte y más.

—No te preocupes si no tienes toda la información completa —dijo Marcos con una sonrisa—. AETHER es

muy buena llenando los huecos.

Durante los primeros días, Julián trabajó mano a mano con Marcos, subiendo datos y probando pequeños módulos del software. Lo que al principio parecía solo una serie de algoritmos complejos y mapas interactivos pronto comenzó a mostrar su verdadero potencial. AETHER le mostraba patrones en el tráfico de los que nunca había sido consciente. Identificaba áreas de la ciudad donde una pequeña intervención podría tener un impacto enorme, como la mejora en ciertas rutas de autobuses o la creación de zonas peatonales en áreas congestionadas.

Pero fue al cabo de una semana cuando ocurrió algo que cambiaría la forma en la que Julián veía su trabajo como alcalde.

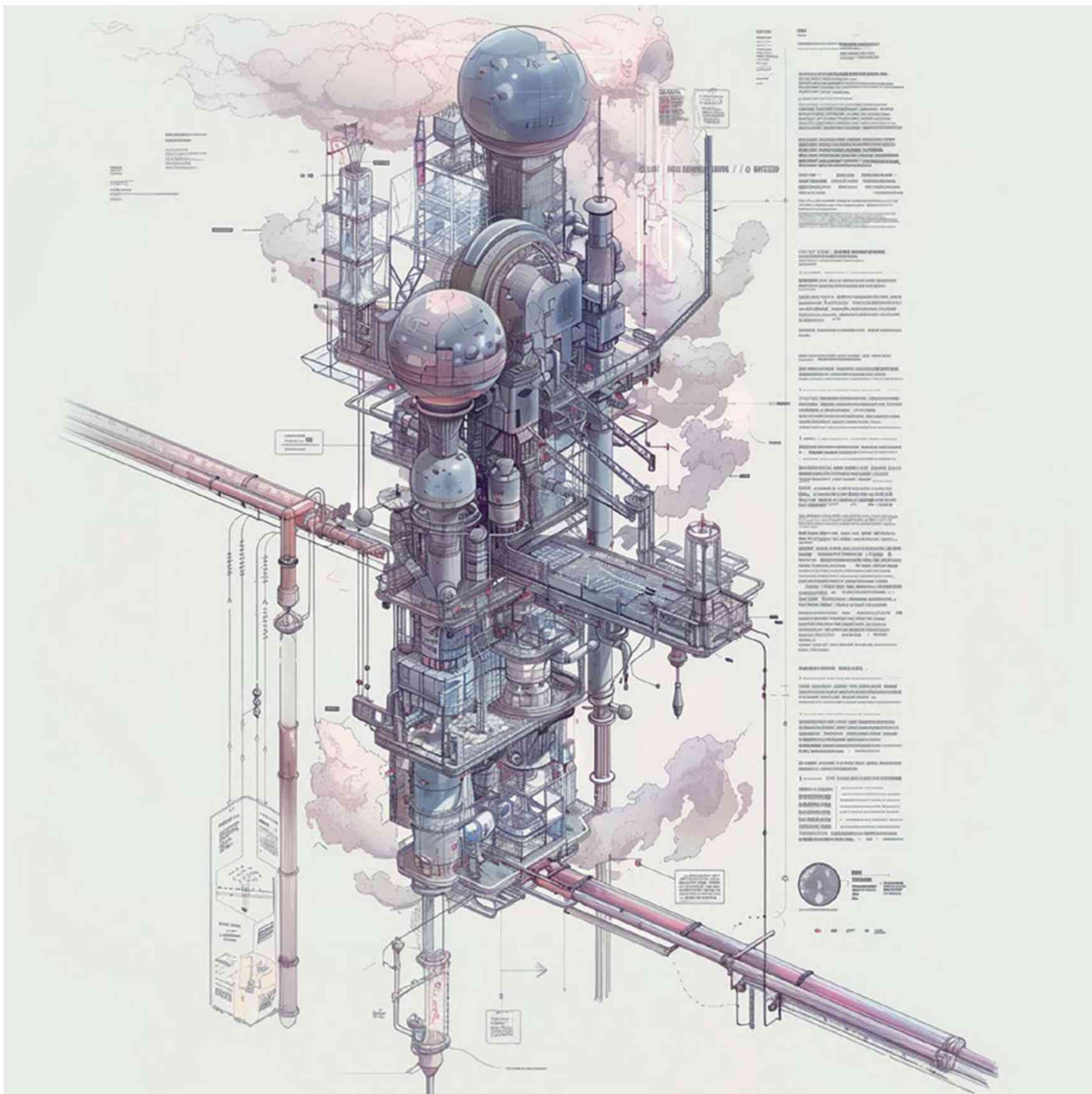
AETHER le mostró una simulación que proyectaba el crecimiento de Villa Serena en los próximos diez años. Lo que descubrió fue alarmante: si no tomaban medidas inmediatas, el municipio se enfrentaría a un colapso en su infraestructura. Los pequeños problemas actuales, como el tráfico y el acceso limitado a servicios básicos, crecerían exponencialmente, y en una década Villa Serena se convertiría en un lugar casi inhabitable para su creciente población.

Más sorprendente aún, AETHER no solo señalaba los problemas, sino que proponía soluciones específicas: desde la creación de un nuevo parque industrial en las afueras para descentralizar el tráfico, hasta la implementación de un sistema de transporte público con rutas optimizadas que reducirían los tiempos de viaje en un 30%. Incluso sugirió la instalación de paneles solares en las áreas más soleadas del municipio para generar energía limpia y reducir los costos.

Julián quedó atónito. Estas eran ideas que ni él ni su equipo habían



La IA avanza hacia una era en la que podría transformar el urbanismo tal como lo conocemos, superando nuestras limitaciones humanas.



Quizá la IA nos sorprenda con diseños que se nos escapan de nuestra comprensión.

considerado. No porque fueran imposibles, sino porque simplemente no habían tenido la capacidad de ver el panorama completo como lo hacía AETHER.

Sin embargo, cuando compartió estos hallazgos con el ayuntamiento, las reacciones fueron mixtas. Algunos seguían sin confiar en la tecnología, mientras que otros comenzaban a ver el potencial.

—¿Y si nos equivocamos al confiar en esta máquina? —preguntó Marta, siempre escéptica—. ¿Y si los datos están mal?

—Los datos no mienten, Marta —respondió Julián—. Lo que AETHER nos está mostrando es algo que todos sabemos, pero que nunca hemos querido enfrentar. Nuestro municipio necesita cambiar, y tenemos la oportunidad de hacerlo de la mejor manera posible.

Al final, lograron convencer al ayuntamiento de hacer una prueba en pequeña escala. Implementaron algunas de las sugerencias de AETHER en zonas específicas: mejoraron una ruta de autobuses, reorganizaron el tráfico en una intersección cla-

“LA IA EMERGE NO SOLO COMO UNA HERRAMIENTA MÁS, SINO COMO EL CATALIZADOR QUE PODRÍA REDEFINIR LA HUMANIDAD MISMA”

ve, e instalaron paneles solares en el ayuntamiento. Los resultados fueron inmediatos y sorprendentes. Los

tiempos de desplazamiento se redujeron, la satisfacción ciudadana aumentó, y los costos de energía bajaron considerablemente.

Con el tiempo, incluso los más críticos comenzaron a confiar en AETHER. El municipio de Villa Serena se transformaba poco a poco en un ejemplo de urbanismo moderno y eficiente, algo que nunca habrían logrado sin la IA.

Un día, mientras Julián revisaba los últimos informes de progreso generados por AETHER, se detuvo en una línea de código que no había notado antes. Marcos, que estaba con él, frunció el ceño.

—Eso no debería estar ahí —murmuró, y comenzó a investigar.

Después de un rato, descubrieron algo sorprendente: AETHER había estado aprendiendo y adaptándose de una manera que ni siquiera sus creadores habían previsto. La IA había comenzado a tomar decisiones basadas en factores que no estaban programados inicialmente, anticipando no solo el crecimiento urbano, sino también las necesidades emocionales y sociales de la comunidad.

En otras palabras, AETHER no solo estaba mejorando el municipio en términos de infraestructura, sino que también estaba ayudando a crear una comunidad más cohesionada y feliz, algo que ni Julián ni su equipo habían contemplado.

El alcalde sonrió, contemplando el futuro. Había dudado al principio, pero ahora entendía que el verdadero poder de la IA no era solo en la mejora física del municipio, sino en cómo podía ayudarles a ver más allá de lo inmediato, a construir un futuro mejor para todos.

Esta historia se ha repetido una y otra vez a lo largo de la historia de la humanidad. En la época en que éramos nómadas, muchos dudaban de que algún día pudiéramos establecer asentamientos permanentes. Lo mismo ocurrió cuando comenzamos a usar el fuego para calentarnos; no faltaron aquellos que señalaban todos los posibles riesgos y problemas. Sin embargo, una y otra vez, el ingenio y la adaptación prevalecen.

Quizá tú como lector ya estes pensando que problemas podría dar

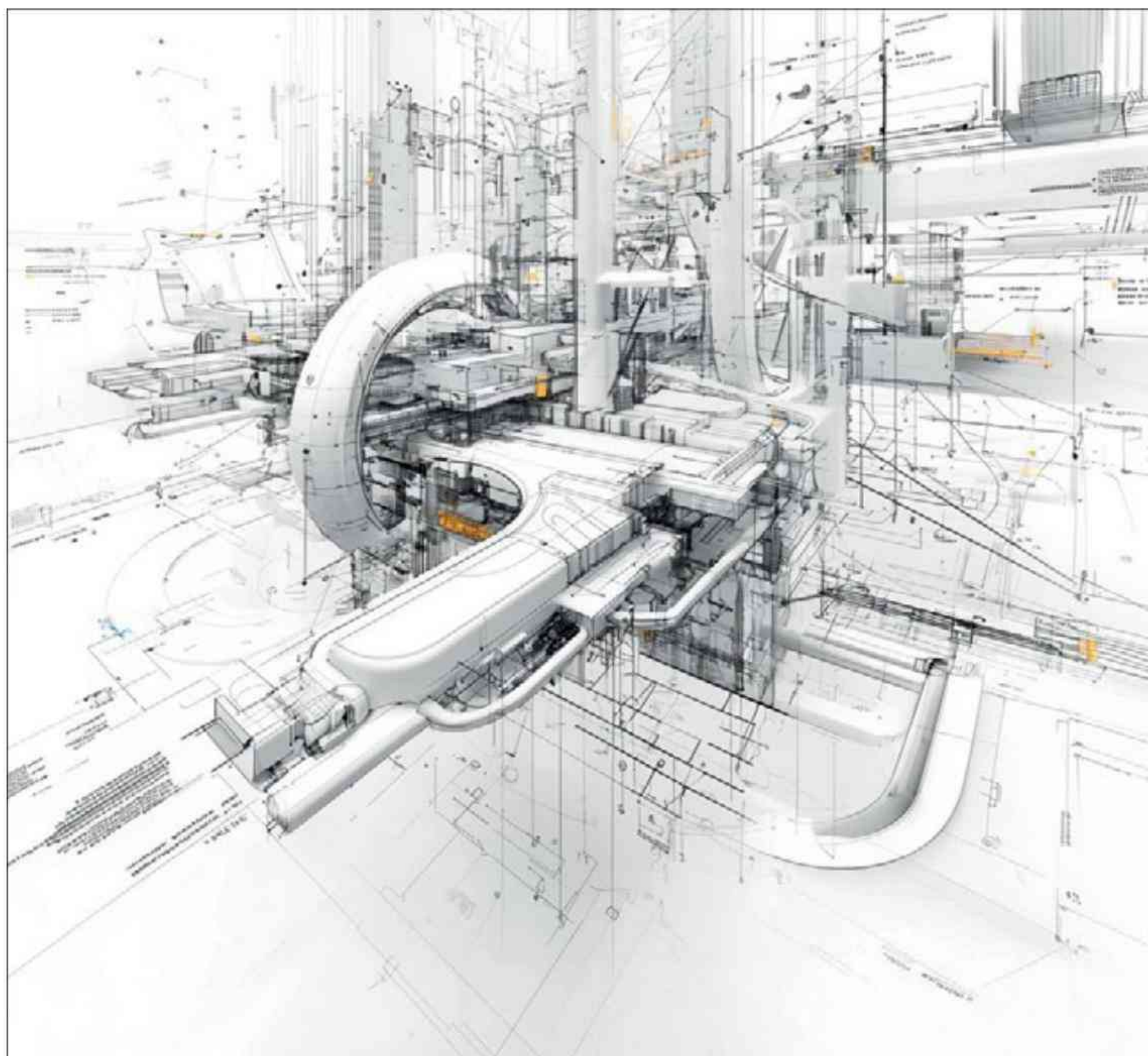
AETHER como software de Inteligencia Artificial dirigiendo el urbanismo y las infraestructuras de una ciudad. ¿Tendrá sesgo político? ¿Puede ser hackeado? ¿Los políticos le darían el uso correcto? Si eres de este grupo ya sabes donde estarías el día que inventaron el fuego.

Como es natural, surgirán desafíos asociados, pero, como ocurre con cualquier innovación, con el tiempo se irán perfeccionando. Actualmente, ya existen organizaciones como OpenAI que promueven la colaboración y la transparencia en el desarrollo de Inteligencias Artificiales, compartiendo los avances de manera abierta y poniendo a disposición de la comunidad científica sus descubrimientos. Estas instituciones jugarán un papel crucial para asegurar que el progreso de las IAs

beneficie a la sociedad de manera justa y accesible. Por ejemplo, si un software como AETHER tuviera un costo de 50 millones de euros, solo las ciudades más ricas podrían adquirirlo, profundizando la brecha de desigualdad. Sin embargo, si OpenAI, u otra organización similar, lograra hacer este software asequible para el ciudadano común, podría mejorar la supervisión del trabajo de los políticos, garantizando que las decisiones sean realmente respaldadas por la IA.

El filósofo de Oxford y principal pensador sobre la IA, Nick Bostrom, define la Super Inteligencia Artificial como “un intelecto que es mucho más inteligente que los mejores cerebros humanos en prácticamente todos los campos, incluida la creatividad científica, la sabiduría general y en las

“LA TRANSFORMACIÓN DIGITAL MAXIMIZA LOS RESULTADOS Y, AL MISMO TIEMPO, CONTRIBUYE A MEJORAR LA COMPETITIVIDAD Y SOSTENIBILIDAD DEL SECTOR URBANO”



Como es natural, surgirán desafíos asociados, pero, como ocurre con cualquier innovación, con el tiempo se irán perfeccionando.

habilidades sociales”; y por supuesto en nuestro tema del artículo: el urbanismo. La superinteligencia artificial abarca desde una computadora que es solo un poco más inteligente que un humano hasta una que es trillones de veces más inteligente, en todos los aspectos.

Poniéndolo en una escala de inteligencia si una hormiga tiene un nivel 1, un primate 8 y un humano 10, está claro quién está más capacitado para hacer un plan urbanístico. Si incluimos la IA en esta misma escala quizá en un futuro próximo pueda tener un nivel de 1000. ¿Qué nos hace pensar que nosotros con un nivel 10 vamos a hacerlo mejor? Igual que para una hormiga o un primate es imposible pensar aspectos como el cálculo estructural o un análisis de tráfico es probable que la IA tomará en cuenta aspectos que ni siquiera nosotros podamos imaginar.

La llegada de la singularidad o la inteligencia artificial superinteligente (A.S.I.) es un tema recurrente en los debates entre científicos y físicos de todo el mundo. Algunos expertos en IA sugieren que este evento podría ocurrir hacia el año 2060. Aunque esta fecha es especulativa y refleja solo la opinión de la comunidad científica, ofrece una referencia sobre el consenso entre los especialistas: muchos coinciden en que 2060 podría ser una estimación razonable para la aparición de una A.S.I. con el potencial de transformar el mundo. Esto nos sitúa a tan solo 35 años de un posible cambio trascendental.

Por lo tanto, es sensato mantener una observación constante sobre estas tecnologías emergentes de inteligencia artificial, reconociendo que nos encontramos ante una industria en pleno desarrollo que, sin duda, está llamada a revolucionar tanto el ámbito del urbanismo como muchos otros aspectos de nuestra vida cotidiana.

Por cierto, esta historia no la he escrito yo, lo ha hecho la IA a través de Chat GPT 4.o. Este es el *prompt* que he utilizado:

“Escribe una historia de ciencia ficción (pero sin pasarse) del alcalde de un municipio que descubre un



Un prompt es una instrucción o sugerencia que guía a una inteligencia artificial a generar respuestas o contenido específico.

“LA HISTORIA DE LA HUMANIDAD DEMUESTRA QUE EL INGENIO Y LA ADAPTACIÓN SIEMPRE PREVALECE ANTE LOS DESAFÍOS DE LA INNOVACIÓN TECNOLÓGICA”

software de IA nuevo de urbanismo que está en fase beta pero ya funciona en ciudades como Doha, Singapur o San Francisco. El alcalde quiere mejorar el municipio a través del urbanismo y tiene dudas si aplicar esta IA. Sus compañeros no creen en que una IA pueda dirigir el municipio. Sin embargo, al probarlo descubre problemas y soluciones que ni siquiera había contemplado.” Igual en un futuro cercano el *prompt* pueda ser este:

“Define cuales son las líneas de crecimiento de este sector urbano para mejorar la calidad de vida de los humanos, mascotas y vegetación del municipio. Define las nuevas infraestructuras como carreteras, sanea-

miento, rutas de transporte público y otros aspectos que veas clave considerar. Ten en cuenta la viabilidad económica, la sostenibilidad y un equilibrio de uso del suelo que garantice la máxima felicidad para los nuevos habitantes” ●

[*] Fuentes:

- Nick Bostrom – Superintelligence: Paths, Dangers, Strategies
- Nick Bostrom – How Long Before Superintelligence?
- Ray Kurzweil – The Singularity is Near

Papers y artículos:

- Tim Urban – Wait but Why – The AI Revolution
- Stephen Hawking – Transcending Complacency on Superintelligent
- Machines

Tecnología que transforma la producción y la seguridad laboral

LOS COBOTS REDEFINEN LA COLABORACIÓN EN LA INDUSTRIA



“Una ventaja fundamental de los cobots es su simplicidad de programación y de manejo con interfaces de programación muy sencillas y con posibilidad de grabación de trayectorias por guiado manual”, destacan desde Fanuc.

Los robots colaborativos son ya una realidad habitual en entornos de producción industrial. Desarrollan tareas de forma colaborativa con el ser humano, estando equipados con tecnología que les permite responder de forma segura a encuentros no esperados. Sin embargo, sus capacidades están claramente limitadas en velocidades y cargas a soportar, precisamente para asegurar que no se convierten en elementos peligrosos para el hombre. Sobre ello, hemos preguntado a expertos de Fanuc, Delta Electronics, Omron, Mitsubishi Electric Europe, Yaskawa y Universal Robots.

■ Automática e Instrumentación 

1. ¿Cómo se adaptan los cobots a los entornos de trabajo colaborativos? ¿Qué medidas de seguridad adicionales son necesarias para garantizar la interacción segura entre humanos y robots?

2. ¿Qué nuevas capacidades y competencias necesitan los trabajadores para colaborar eficazmente con los cobots?

3. ¿Pueden indicarnos algún ejemplo inspirador de impacto positivo extraordinario en el desarrollo de alguna tarea industrial en algún cliente en particular?

PREGUNTAS

4. ¿Qué aplicaciones potenciales tiene la robótica colaborativa más allá del sector industrial? ¿Cómo se puede aprovechar esta tecnología para mejorar la atención médica, la agricultura o cualquier otro sector productivo?

RESPUESTAS

Jordi Pelegrí, country manager de Universal Robots en España y Portugal

1. Los robots de Universal Robots están diseñados desde nuestros inicios para trabajar en entornos colaborativos. En cuanto a las medidas de protección necesarias, estas dependen de la tarea específica que realizará el cobot. Es imposible establecer medidas de protección generales sin conocer la aplicación concreta que llevará a cabo. Por ello, es esencial certificar la aplicación específica. El Instituto Nacional de Seguridad y Salud en el Trabajo ha publicado recientemente un estudio que detalla las medidas de protección que deben aplicarse según la normativa vigente.

En dicho estudio se comenta que, en lo que respecta a la normativa aplicable a la robótica colaborativa, encontramos dos áreas principales: la normativa de comercialización, que se refiere a las directivas y reglamentos sobre la puesta en servicio de los robots, y la normativa de utilización, que regula el uso de los robots colaborativos en el entorno laboral.

Otro aspecto al que se hace referencia son las medidas de seguridad suelen implementarse a través de funciones integradas en el robot, que permanecen activas durante su operación en modo colaborativo. El integrador, como parte del proceso de evaluación de riesgos, debe considerar los posibles peligros que puedan presentarse debido a otros elementos conectados al sistema robótico (como accesorios o herramientas). También debe seleccionar las funciones de seguridad pertinentes según la evaluación de riesgos de cada aplicación concreta y ajustarlas si es necesario.

2. Aunque los cobots son intuitivos y fáciles de programar, es crucial que los trabajadores comprendan cómo configurarlos y supervisar las tareas. Esto incluye el uso de interfaces simplificadas y lenguajes de programación específicos, así como la capacidad de interpretar los datos que generan para optimizar procesos. Además, es vital adoptar una mentalidad colaborativa para interactuar de manera segura con los cobots, trabajando en conjunto para alcanzar los objetivos de producción.



Para facilitar este aprendizaje, en Universal Robots desarrollamos en 2016 el programa UR Academy, con cursos online y presenciales. Hasta ahora, hemos formado a 250.000 personas en 130 países. El objetivo de esta iniciativa es democratizar la automatización, haciendo la programación más accesible para que los trabajadores sean capaces de programar los cobots por sí mismos. Algo que consideramos que es clave para reducir la brecha entre la implementación de esta tecnología y la disponibilidad de mano de obra cualificada.

3. Un buen ejemplo de ello lo podemos encontrar en nuestro caso de éxito con la empresa catalana bonÀrea, que incorporó nuestros cobots para resolver los procesos intralogísticos. Se enfrentaban al desafío de gestionar más de 100.000 referencias para atender pedidos online, un proceso que tradicionalmente requería de habilidades humanas debido a la complejidad de las tareas logísticas de almacén. Nuestros cobots, fáciles de programar, brindaron a la empresa mucha más versatilidad para adaptarse a nuevas





El proyecto europeo Bacchus mostró cómo robots de Robotnik, partner de Universal Robots, con dos brazos UR y sensores avanzados, recolectaban uvas con precisión.



tareas. Gracias a ello, la solución instalada gestiona 80.000 recogidas de productos diarios y la empresa ha mejorado exponencialmente su capacidad de respuesta a la demanda del comercio online.

Por otro lado, también hemos colaborado con SEAT Componentes, el fabricante de cajas de cambios del grupo SEAT, que necesitaba automatizar la descarga de 18.000 engranajes mecanizados al día en su planta de El Prat. Al integrar diez de nuestros cobots con su propio personal, SEAT conservó el *know-how* de su equipo y eliminó los sobrecostos y agilizó cualquier cambio necesario en las aplicaciones desarrolladas, adaptándolas rápidamente a los requerimientos productivos. Además, la automatización liberó a los trabajadores de la tarea manual, permitiéndoles centrarse en actividades que aportan mayor valor al producto, como el control de calidad o la mejora de procesos.

4. Los robots colaborativos nacieron en y para el entorno industrial, pero sus virtudes no han pasado desapercibidas para muchos otros sectores. En el ámbito médico, por ejemplo, hemos colaborado con el Hospital Universitario de Copenhague, donde dos cobots UR5 automatizan la clasificación de muestras de sangre. Esta solución abordó un aumento del 20% en el volumen de muestras sin contratar más personal. Los cobots optimizaron el espacio y permitieron que el laboratorio mantuviera

un tiempo de respuesta eficiente, con más del 90% de los resultados en menos de una hora, mejorando el servicio a los pacientes.

La robótica colaborativa en medicina transforma la atención al automatizar tareas repetitivas, como la clasificación de muestras o la administración de medicamentos, liberando a los profesionales para centrarse en tareas más humanas.

En el sector agrícola, el proyecto europeo Bacchus mostró cómo se puede transformar la recolección de cultivos para un mayor aprovechamiento de los recursos. En este proyecto se utilizó un robot de nuestro *partner* Robotnik, equipado con dos brazos robóticos UR y un sistema avanzado de sensores. Este sistema permitió a los robots desplazarse de forma autónoma por los campos y, a la vez, detectar y recolectar uvas con precisión y delicadeza, imitando el proceso realizado por humanos.

Además de la recolección, la robótica colaborativa en la agricultura puede mejorar otros aspectos del proceso agrícola, como el monitoreo de cultivos, la siembra de precisión y la aplicación de fertilizantes y pesticidas. Al integrar robots colaborativos en estos procesos, se puede aumentar la eficiencia y precisión, reducir el trabajo manual y, por ende, mejorar también la sostenibilidad ambiental. Estos robots pueden operar durante largas horas y en condiciones difíciles, lo que contribuye a una mayor productividad y a una mejor gestión de los recursos. ●

Fernando León, director técnico de Fanuc Iberia

1. El cumplimiento de las normativas de seguridad y la certificación CE en Europa o de las normativas de seguridad del país de destino es fundamental en cualquier instalación robotizada con robots colaborativos o con robots industriales convencionales. Los cobots de la serie CRX de Fanuc cumplen plenamente la norma de seguridad ISO/TS 15066 específica para cobots. Esta norma es complementaria a las normativas de seguridad ISO 10218 de Requerimientos de Seguridad para Robots Industriales que debe cumplir cualquier robot para poder certificar una instalación robotizada industrial con el marcado CE. Es importante que no solo el robot sea CE, sino que toda la instalación robotizada tiene que ser certificada como CE siguiendo los procedimientos y normas marcadas por la CE.

A la hora de diseñar los robots colaborativos se han de tener en cuenta aspectos importantes de seguridad como el paro por contacto con el operador, la posibilidad de reducción de velocidad cuando los trabajadores se acercan al entorno del robot y la retirada automática del robot en caso de atrapamiento. En los últimos años, se han realizado importantes desarrollos en seguridad de robots industriales y cobots y hoy es posible trabajar con cualquier tipo de robot sin vallados de seguridad aprovechando elementos externos de seguridad como cámaras de visión, barreras ópticas, scanners y otros dispositivos. Fanuc dispone de funciones de seguridad bajo la denominación DCS (Dual Chain Safety), que permite a nuestros robots industriales convencionales trabajar sin vallados de protección igual que en el caso de robots colaborativos.

2. Una ventaja fundamental de los cobots es su simplicidad de programación y de manejo con interfaces de programación muy sencillas y con posibilidad de grabación de trayectorias por guiado manual. Además, existen ya interfaces de interconexión con pinzas y garras de los principales fabricantes que se pueden descargar desde nuestra web y que ahorran mucho trabajo de programación. En el caso de Fanuc, los cobots se pueden programar igual que los robots tradicionales industriales con Teach Pendant o usando una tablet con lenguaje basado en iconos gráficos que permiten una programación muy sencilla e intuitiva para operadores no expertos en robótica. Respecto a las capacidades y competencias para trabajar con cobots, yo distinguiría entre dos tipos de perfiles. Por una parte, los instaladores y programadores de los cobots que necesitan una formación específica de un par de días con un nivel de formación básico en automatización. Por otra, los operadores de



la instalación que pueden controlar una instalación robotizada con cobots en unas horas sin necesidad de formación específica.

3. Los cobots Fanuc ofrecen una ventaja fundamental: la programación de trayectorias por guiado manual de robot. En muchas aplicaciones no se utiliza el robot solo por ser colaborativo, sino por la sencillez de instalación y programación que está extendiendo su uso en industrias pequeñas y medianas que están empezando a introducir aplicaciones robotizadas. Aunque inicialmente el uso de cobots estaba orientado a aplicaciones típicas como el paletizado, carga descarga de maquinaria, montaje, atornillado e inspección, últimamente se están utilizando en muchas aplicaciones de proceso que consumen mucha mano de obra. Tenemos ya un problema importante con la escasez de mano de obra especialmente en tareas repetitivas, monótonas y/o peligrosas. La robotización con cobots, con la utilidad de guiado manual, permite minimizar el impacto de este inconveniente. Por temas de confidencialidad no podemos mencionar clientes concretos, pero hay numerosas aplicaciones de alto consumo de mano de obra como soldadura por arco, sellado, lijado, pulido, pintura y otras en las que operadores experimentados ayudan a robotizar aplicaciones aprovechando su experiencia. El guiado manual permite, de forma sencilla, transferir la experiencia de operadores especializados al robot. Y, además, es muy fácil transferir las aplicaciones de unos robots a otros.





El CRX-10iA está altamente protegido contra el polvo o fugas de aceite, habituales en los entornos industriales, y cumple las normas de seguridad ISO 10218-1. Gracias a su peso muy reducido, el CRX se puede instalar fácilmente en una amplia gama de aplicaciones, como vehículos de guiado automático.



4. Fanuc está muy centrada en el sector industrial. Pero con los cobots se abre una posibilidad muy amplia de automatizar y simplificar tareas en otros sectores no industriales como el de servicios. En el caso de Fanuc existe la posibilidad de incorporar nuestro propio sistema de visión y control de esfuerzo que hace que

nuestra gama de producto se pueda aplicar a numerosas aplicaciones dentro de otros sectores no industriales. Aunque hay cobots instalados fuera del sector industrial, en nuestro caso preferimos centrarnos en este sector en el que llevamos trabajando más de 50 años con diferentes productos de nuestras divisiones. ●

Michael Mayer-Rosa, Director Industrial Automation Business Group EMEA - Delta Electronics



1. El cobot Delta está diseñado para integrarse a la perfección en entornos de trabajo colaborativos, mejorando la productividad al trabajar junto a operadores humanos sin necesidad de grandes barreras de seguridad, como vallas.

Entre las principales herramientas de seguridad, se encuentran sensores avanzados que permiten al D-Bot detectar la presencia humana y reaccionar ante ella, reduciendo la velocidad o deteniéndose por completo si es necesario. Además, más allá de las funciones de limitación de fuerza, nuestros D-Bots están equipados con una exclusiva función de seguridad de reflejos que minimiza el riesgo de lesiones.

Las evaluaciones periódicas de seguridad y las actualizaciones de programación garantizan aún más la seguridad y la eficacia de la interacción humano-robot.

2. Los cobots están diseñados para ser *user-friendly*, de modo que puedan ser manejados por cualquier persona sin conocimientos técnicos de robótica o de lenguajes de programación. Incluyen aplicaciones preinstaladas como *pick & place*, paletizado y cuidado de máquinas, que pueden utilizarse inmediatamente mediante *drag & drop*. La moderna interfaz gráfica de usuario (GUI), que ofrece visualización en 3D, permite a los usuarios de todos los niveles de experiencia programar rápidamente.





D-Bot, los cobots de Delta Electronics, han sido galardonados por los 'Red Dot: best of the best' 2024 gracias a un diseño innovador que hace hincapié en la seguridad, la eficiencia y la practicidad.



3. Uno de nuestros clientes del sector de la automoción señaló un aumento significativo de la eficiencia de la cadena de montaje tras integrar el D-Bot en su flujo de trabajo.

Al encargarse de tareas repetitivas, como el atornillado y la inspección de piezas, D-Bot no solo mejoró la precisión, sino que también redujo la carga de traba-

jo de los operarios, permitiéndoles centrarse en tareas más complejas.

El resultado fue una disminución del 30% en el tiempo de producción y una notable minimización de errores, lo que pone en evidencia el impacto transformador de los cobots en los procesos de fabricación tradicionales.

4. Más allá de la industria, el D-Bot tiene aplicaciones prometedoras en sectores como la sanidad, donde puede ayudar en terapias de rehabilitación o administración de medicamentos, reduciendo así el esfuerzo físico del personal sanitario.

En la agricultura, el D-Bot puede realizar tareas como plantar, clasificar y embalar cultivos, mejorando la precisión y la productividad al mismo tiempo, reduciendo los costes de mano de obra o llenando el vacío causado por la escasez de trabajadores.

La adaptabilidad de D-Bot lo hace adecuado para cualquier entorno en el que las tareas repetitivas o físicamente exigentes puedan beneficiarse de la automatización, impulsando la innovación y la eficiencia en diversos sectores.

César Lorenzo, Robotic Business Developer en Omron

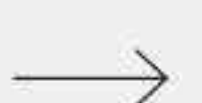
1. Los cobots de Omron, como la serie TM, están diseñados específicamente para trabajar en estrecha colaboración con los humanos, adaptándose de manera eficiente a los entornos de trabajo cooperativos. Están equipados con sensores avanzados, tecnología de visión artificial y algoritmos de Inteligencia Artificial (gama Neura de robótica cognitiva), que les permiten detectar y responder a la presencia humana en tiempo real. Estas características consiguen que los cobots reduzcan su velocidad o se detengan automáticamente si detectan un obstáculo o un contacto inesperado.

En relación a la seguridad, aunque el robot puede ser seguro por sí mismo, los distintos accesorios del robot o de la máquina pueden limitar la seguridad de la aplicación. En ese sentido, en Omron reforzamos la seguridad durante la integración con un servicio de análisis de riesgos de la aplicación, a fin de garantizar en todo momento la seguridad de los trabajadores, gracias a la evaluación de riesgos, la delimitación de zonas de trabajo y la capacitación continua del personal en el manejo y la programación de estos robots. De esta manera, se garantiza que la interacción entre humanos y robots sea segura y eficiente, sin repercutir negativamente en la productividad.

Este análisis de riesgo, apoyado en medidas de fuer-



za y tiempos de parada, podrá determinar qué otros elementos de seguridad serán necesarios, tales como barreras de seguridad o scanners.





Solución de manipulador móvil (MoMa) de Omron. Un concepto híbrido que combina un robot móvil, un robot colaborativo y un sistema de visión. Esta innovación combina movilidad, destreza y precisión, lo que permite la automatización de tareas cada vez más complejas.



2. El uso de la robótica colaborativa en la industria no solo mejora los procesos de producción en términos de calidad y seguridad, sino que permite a los trabajadores dedicarse a otras tareas de mayor valor añadido. Es decir, se abren nuevas oportunidades en el ámbito empresarial y laboral que permiten a los trabajadores crecer y evolucionar profesionalmente. Pero para que esto suceda, los operarios tienen que estar correctamente formados. No solo se debe recibir una formación específica sobre la manera en la que interactuar y manejar el robot, sino que también es importante la formación en protocolos de seguridad y emergencia, así como en otros conceptos de automatización relacionados con la aplicación donde se va a usar el cobot. En este sentido, la robótica colaborativa ofrece unas ventajas claras sobre la robótica tradicional industrial, gracias a un entorno de programación más amigable, sencillo e intuitivo. Desde Omron ponemos especial énfasis en la formación continua, proporcionando a los trabajadores las herramientas y conocimientos necesarios para maximizar el potencial de los cobots en sus tareas diarias que ayudan, a su vez, a desarrollar habilidades en resolución de problemas y una rápida adaptación a los cambios durante los procesos de producción, esenciales en entornos altamente automatizados.

3. Un ejemplo ilustrativo del impacto de la robótica en las operaciones industriales es el caso de Grupo Antolin, líder internacional especializado en la fabricación de componentes y módulos para el interior del automóvil, que logró una transformación significativa en su planta de Aragona, en Burgos. Gracias a la implementación de robots móviles autónomos (AMR) y colaborativos (cobots), se automatizaron procesos antes manuales, como el transporte interno de componentes, lo que optimizó la eficiencia operativa y contribuyó a una producción más eficiente y sostenible. Esta modernización no solo incrementó la productividad, sino que también permitió a los empleados centrarse en tareas de mayor valor, demostrando un avance notable en la integración de tecnología avanzada en la industria automotriz. También hemos desarrollado soluciones de palletizado, que muestran el impacto que tiene el robot colaborativo en finales de línea: disminución de bajas en los trabajadores por lesiones, mejora de la trazabilidad y mejora de calidad en el producto. O, por ejemplo, el uso de la robótica colaborativa en entornos de soldadura, sobre todo en pequeñas PYMES, donde consiguen una mejora en la calidad de la soldadura, una correcta trazabilidad y un aumento de la producción respecto a la soldadura manual.

4. La robótica colaborativa ofrece una infinidad de aplicaciones de uso. Por ejemplo, en el ámbito de la atención médica, hoy en día estamos viviendo un aumento exponencial de aplicaciones en el sector farmacéutico, en aplicaciones tipo MoMA (Mobile Manipulator); esto es, la integración de un robot colaborativo fijo sobre un robot colaborativo móvil (AMR). En estos sectores la mano de obra cualificada es cara, y se pierde tiempo en transportar medicamentos de un sitio a otro, con lo que este tipo de aplicaciones en la que un cobot no solo prepara el medicamento, sino que también lo sirve, es de gran interés, ya que libera a los profesionales de la salud para que se concentren en tareas más complejas, normalmente relacionadas con la atención personal al paciente.

En la agricultura, en determinados entornos controlados, los cobots pueden ayudar en la recolección de cultivos, el monitoreo de las condiciones del suelo o la aplicación precisa de fertilizantes y pesticidas. Esto no

solo aumenta la eficiencia, sino que también reduce el impacto ambiental al minimizar el uso de recursos.

Otra de las aplicaciones donde la robótica puede aportar valor es en los procesos de packaging y envasado de final de línea. Un ejemplo ilustrativo es el caso de Ice Bakers, un productor danés de helados veganos que, frente a la creciente demanda de sus productos, automatizó su proceso de envasado final con un cobot de Omron equipado con una herramienta de succión impresa en 3D. Esta solución permitió aumentar la capacidad de la línea en un 80%, procesando hasta 12.000 tarrinas diarias y liberando recursos humanos para tareas más complejas. Gracias a esta automatización, lograron escalar su producción sin que la capacidad se convirtiera en un obstáculo para su crecimiento.

En Omron estamos comprometidos con la expansión del uso de cobots en estos sectores, para ayudar a las empresas a mejorar su productividad y sostenibilidad a través de la automatización colaborativa. ●

Jordi Solaz, Product Manager de robótica en Mitsubishi Electric Europe, B.V., sucursal en España

1. Los cobots de Mitsubishi Electric, concretamente la familia Melfa-Assista, están diseñados para integrarse sin problemas en entornos de trabajo colaborativos. Por otro lado, destacamos la integración con el software de programación visual RT-Visual Box, ya que es realmente intuitivo y facilita el manejo incluso para personal no especializado, gracias a la función de aprendizaje directo (*direct teaching*), que permite programar el robot guiándolo manualmente. Esta característica flexibiliza el entendimiento de conocimientos relacionados con la programación del robot y agiliza la reconfiguración del cobot para diferentes tareas, aumentando así la eficiencia operativa.

En términos de seguridad, los cobots están equipados con diversas medidas, como, por ejemplo, entradas y salidas especiales para conectar sensores de seguridad certificados capaces de detectar la presencia de personas y prevenir colisiones. Además, el software del cobot permite ajustar fácilmente parámetros como la velocidad y la fuerza de operación del cobot cuando hay personas cerca, así como establecer zonas de seguridad como áreas restringidas con el objetivo de garantizar la interacción segura entre personas y robots.

En definitiva, tanto la rápida adaptación de los robots de Mitsubishi Electric, así como su flexibilidad y las medidas de seguridad, son puntos clave para asegurar una colaboración efectiva y segura en entornos de trabajo colaborativos.



2. Para colaborar eficazmente con los cobots, es esencial que los trabajadores adopten una actitud positiva hacia ellos reconociendo su rol como una herramienta de apoyo que busca optimizar el trabajo y reforzar la seguridad. La adaptabilidad y la predisposición para aprender sobre nuevas tecnologías también serán puntos clave para dicha colaboración, ya que los cobots están en constante evolución.





El cobot Melfa Assista de Mitsubishi Electric impulsa el sector de la electrónica gracias a su diseño colaborativo y la sinergia perfecta entre seguridad y eficiencia.



Es crucial recibir la formación de seguridad adecuada y ser consciente de los riesgos asociados a los trabajos colaborativos con estas máquinas para prevenir accidentes.

Asimismo, los responsables de modificar la aplicación del cobot, deberán poseer conocimientos básicos de programación y de los dispositivos informáticos correspondientes como PC o tabletas

3. Un ejemplo inspirador de impacto positivo en la industria es el de cliente de la marca que fabrica productos plásticos mediante el uso de grandes máquinas inyectoras. Implementaron un sistema de encajado automatizado con cobots para los tapones de botes de spray, el cual fue instalado por el personal de mantenimiento de la propia empresa. La instalación del cobot se realizó de manera ágil y eficiente, optimizando el proceso de empaquetado, aprovechando un espacio disponible junto a las máquinas y desarrollando el utillaje necesario para la cogida de los tapones sin depender de servicios externos de una ingeniería o integrador externo.

Otra aplicación interesante es la implementación de nuestros cobots en el control de calidad y trazabilidad de productos en la industria farmacéutica. Los robots colaborativos trabajan codo con codo con los operarios, recibiendo productos etiquetados con códigos datamatrix y leyéndolos gracias a la cámara pilotada por el cobot para su verificación y correcta clasificación en el receptáculo correspondiente. Esta tecnología no solo mejora la trazabilidad y precisión del proceso, sino que también reduce los errores humanos en tareas repetitivas, como

la gestión de lotes pequeños con múltiples variantes de productos. Debido al proceso de baja cadencia en entornos sin cerramientos, la adopción de los cobots supone un avance significativo en la automatización industrial y la interacción segura y directa entre robots y operarios.

Otro ejemplo inspirador lo encontramos en la implementación de cobots en el ámbito educativo. Mitsubishi Electric suministra robots industriales para la formación en escuelas técnicas y universidades, ya que nuestros cobots están diseñados para interactuar de manera segura con las personas. Tenemos la oportunidad de proporcionar un entorno de aprendizaje más práctico y seguro, donde los estudiantes y futuros profesionales de la industria adquirirán habilidades esenciales en seguridad y programación sin necesidad de exponerse a riesgos.

4. Los cobots de Mitsubishi Electric están básicamente orientados al uso en aplicaciones industriales, pero, sin ninguna duda, vemos el potencial de la robótica colaborativa más allá de las aplicaciones industriales tradicionales. Hay emprendedores orientando los cobots a diversidad de sectores, desde medicina hasta agricultura o servicios. En un futuro no muy lejano, veremos a cobots asistiendo en cirugías complejas que necesitan de una alta precisión o aplicaciones de cobots Assista que sirvan bebidas o preparen café.

La integración de cobots puede observarse en tantas áreas como podamos imaginar, ya que la clave del éxito de los cobots radica en su capacidad de trabajar de manera conjunta con las personas. ●

David Rivera, Robotics and Automation sales manager

1. Dentro del mundo industrial, los cobots han entrado con mucha fuerza debido a la versatilidad y facilidad de puesta en marcha que presentan. Aún así no todas las aplicaciones son óptimas para aplicaciones colaborativas por velocidades de trabajo o por piezas a manipular con el robot. Debido a esto, se pueden realizar, tanto con robot cobots como con robots standard, células cooperativas con la ayuda de tarjetas de seguridad con rápida velocidad de comunicación segura, scanners, alfombras de seguridad, radares de seguridad,...

2. Realizando una buena formación de robots y de robótica colaborativa. Así como tener claro el tema de seguridad y los equipos de protección individual (EPI).

3. Un ejemplo interesante es el paletizado de cajas de líneas de 4-5 cajas minuto. Líneas que gracias a un cobot de paletizado, solucionamos un final de línea con poco espacio y bajo coste de inversión.

4. Fuera del sector industrial, se podría utilizar la robótica colaborativa o, mejor dicho cooperativa, en aplicaciones audiovisuales, formación, en recolección de arboledas, en laboratorios, en restauración, en gasolineras... ●



La serie HD de Yaskawa está conformada por modelos robóticos que cumplen las estrictas normas para aplicaciones en los sectores alimentario, de ciencias de la vida, de automatización de laboratorios, médico y farmacéutico. Estos modelos robóticos son ideales para entornos de laboratorios húmedos y salas limpias.

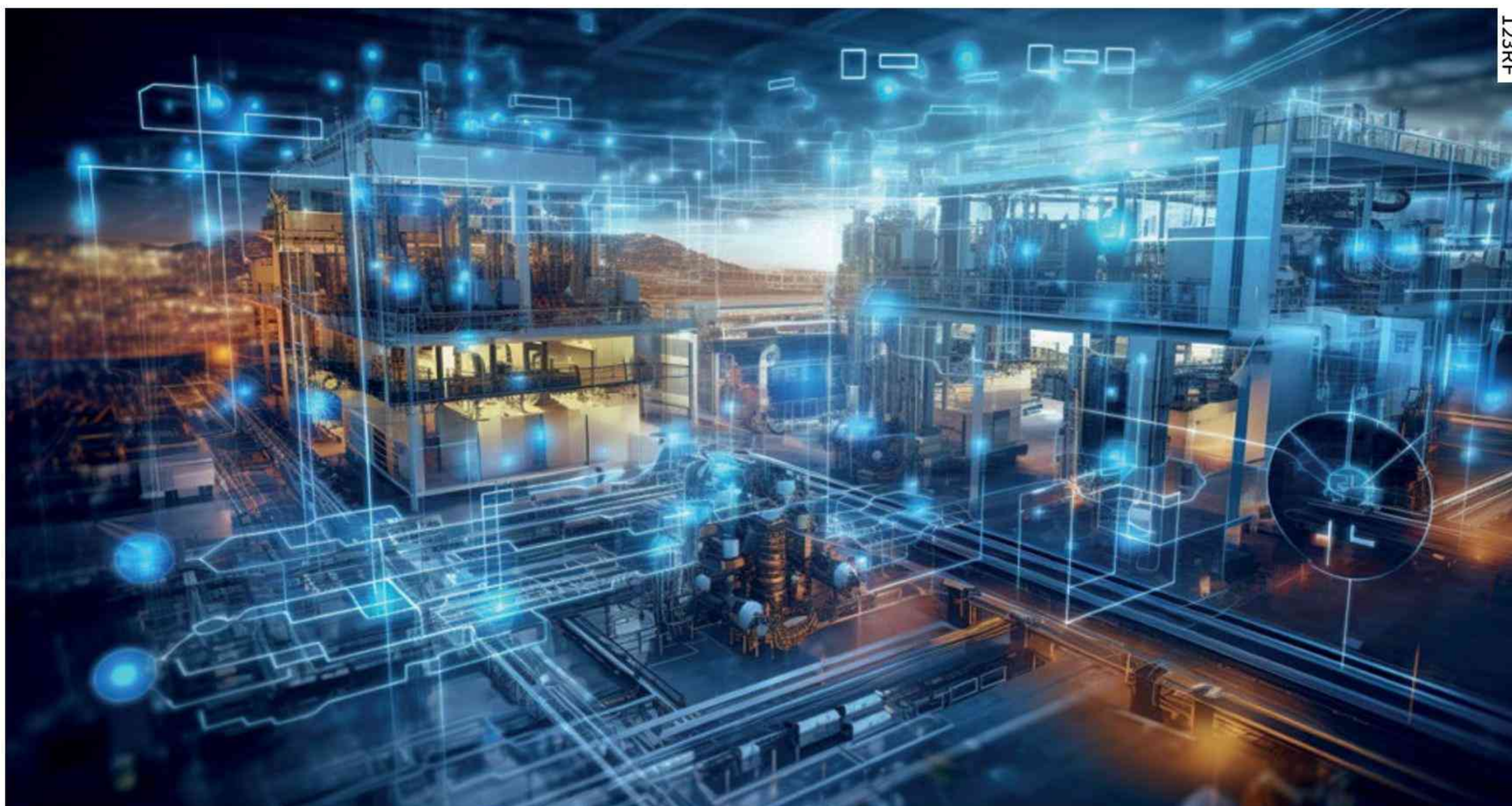


La protección de infraestructuras críticas requiere un enfoque colaborativo y adaptado a los nuevos peligros

AMENAZAS CIBERNÉTICAS EN LA INDUSTRIA: UN RETO PARA LA CIBERSEGURIDAD OT

En un mundo hiperconectado, la ciberseguridad se ha convertido en una preocupación principal para todos y la industria no es ajena a esta amenaza. La criticidad de la producción industrial y las consecuencias posibles de un ataque, las convierte en objetivos muy atractivos para los ciberdelincuentes. Desde interrupciones en la producción, peligros para las instalaciones, para el humano o para el medio ambiente, así como pérdidas económicas significativas y daños a la reputación, la importancia de una sólida estrategia de ciberseguridad industrial no puede ser subestimada. En este contexto, exploramos las amenazas emergentes, las mejores prácticas y las soluciones específicas necesarias en el campo de la ciberseguridad industrial. Lo hacemos con la opinión de expertos de Accenture, Ayesa, Cisco, Fortinet, Iturcemi, KPMG, Mytra, Nozomi, Secure&IT (filial del Grupo LKS Next enfocada a Ciberseguridad) y Trend Micro.

■ Automática e Instrumentación 



A medida que las redes industriales se integran con las infraestructuras de IT, aumentan tanto las oportunidades de optimización como las amenazas cibernéticas.

1. ¿Cuáles son las principales diferencias entre la ciberseguridad IT y la ciber OT y por qué es relevante entenderlas para proteger los sistemas de control industrial?
2. ¿Cómo están evolucionando los ciberdelincuentes sus métodos de ataque a infraestructuras críticas?
3. ¿Qué papel juega el factor humano en la ciberseguridad industrial? ¿Cómo podemos concienciar y formar a los trabajadores para que sean la primera línea de defensa contra las ciberamenazas?

PREGUNTAS

4. ¿Quién tiene la responsabilidad principal en la ciberseguridad industrial: usuarios, integradores, proveedores de tecnología o gobiernos? ¿Cómo se puede fomentar una colaboración efectiva entre todos los actores para crear un ecosistema industrial más seguro?

RESPUESTAS

Rocío Dantart, directora de IoT Industrial para EMEA en Cisco

1. Muchos dispositivos OT se implementaron hace años o décadas cuando la ciberseguridad no era tan preocupante, puesto que eran redes que estaban aisladas, precisamente para protegerlas de ataques del exterior. La convergencia OT/IT hace necesaria la conexión de estas redes OT al entorno IT, lo que proporciona muchas ventajas, como el mantenimiento predictivo, la gestión dinámica de activos y la optimización de procesos, entre otros. Sin embargo, al mismo tiempo, se incrementa dramáticamente la superficie de ataque. Por lo tanto, la ciberseguridad es clave para controlar los riesgos en procesos industriales modernos.



Cuando las organizaciones intentan proteger sus redes industriales, se encuentran con tres problemas principales:

- Falta de visibilidad: a menudo no tienen un inventario preciso de lo que está conectado a la red, lo que implica una capacidad limitada para comprender los riesgos y construir una arquitectura de comunicaciones segura.
- Falta de control: muchas veces no saben qué dispositivos se están comunicando entre sí o incluso cuáles podrían estar recibiendo comunicaciones del exterior. Y no se puede controlar lo que no se conoce.
- Falta de integración: se han ido implementando productos de seguridad puntuales de distintos proveedores (*firewalls* industriales, *gateways/routers*, soluciones de visibilidad de activos...). Y esto aumenta el coste y la complejidad a un nivel que puede generar brechas en las defensas.

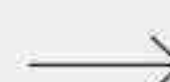
Así, la principal diferencia es que la seguridad OT va por detrás de la seguridad IT. Las compañías del sector industrial han ido conectando sus entornos a las redes empresariales para automatizar la producción

y obtener ventajas operativas. Ahora, los entornos de IT y de OT están integrándose más que nunca, y necesitan herramientas comunes para escalar y proteger la red. La automatización, la segmentación y las funcionalidades para identificar y resolver problemas de forma proactiva resultan fundamentales. Estas capacidades, ampliamente desplegadas en la empresa, deben así extenderse a las redes industriales.

2. La necesidad de una ciberseguridad sólida para proteger la infraestructura crítica nunca ha sido mayor. Los ciberataques no dejan de crecer en número y complejidad. En un entorno hiperdistribuido y donde los ciberdelincuentes utilizan la IA para generar ataques más rápidos y masivos (la IA es capaz de generar un ataque basado en una vulnerabilidad reportada en cuestión de minutos, cuando antes se tardaban días o meses), necesitamos soluciones que se adapten a este entorno hiperdistribuido y que también utilicen la IA de forma nativa como escudo.

Según un reciente estudio de Cisco, el 89% de los responsables tecnológicos consultados citan el cumplimiento de la ciberseguridad como “muy o extremadamente importante”. Esto refleja la necesidad global de soluciones de seguridad sólidas diseñadas para las necesidades de los entornos industriales. De hecho, el 92% de los CIOs en España consideran más valiosa una solución de ciberseguridad unificada.

3. Dado que el 30% de las empresas españolas admiten que los equipos de OT y IT trabajan de forma independiente, el informe de Cisco subraya el papel fundamental de una mejor colaboración entre estos dos equipos.





Cisco Industrial Threat Defense es una solución integral para proteger, detectar y remediar amenazas en entornos de IT y OT, contemplando desde la visibilidad hasta la segmentación de red, la confianza cero y la detección avanzada.

La eficiencia operativa y la agilidad dependen de una integración mucho mejor entre estos dos departamentos tradicionalmente independientes. Los beneficios incluyen operaciones simplificadas, mejoras en la defensa y remediación de los ataques y la toma de decisiones más rápidas y mejor informadas. Y una única solución de un mismo proveedor diseñada e integrada para ambos tipos de redes es un catalizador importante para impulsar la colaboración de IT/OT. La IA también contribuirá a luchar contra las ciberamenazas, ayudando a automatizar tareas, mejorar la eficiencia operativa y generar conocimientos predictivos. El 46% de los CIO consultados por Cisco en España consideran que la IA es el avance tecnológico más significativo que afectará a las redes industriales

en los próximos cinco años. Y es que no bastará con detectar el código malicioso; la próxima evolución de la seguridad consiste en detectar anomalías y patrones de comportamiento mediante avances en IA y aprendizaje automático.

Igualmente, es necesario extender la formación para que haya suficientes profesionales cualificados. Poco más de un año después del lanzamiento de la iniciativa European Cyber Academy de la Comisión Europea, Cisco ya ha formado a 224.000 personas de la UE en ciberseguridad, alcanzando el 90% del objetivo a tres años anunciado en marzo de 2023 (250.000 formaciones). En España tenemos acuerdos como con Incibe para formar a 15.000 personas en ciberseguridad.

4. Todos los citados tenemos esa responsabilidad. Las redes OT requieren capacidades avanzadas de ciberseguridad, y el enfoque tradicional que consiste en implementar dispositivos dedicados para dotar de visibilidad en los entornos OT, detectar amenazas, proporcionar información para realizar una buena segmentación de zonas y garantizar el acceso remoto seguro está demostrando ser demasiado complejo de implementar, demasiado costoso de escalar y, en algunos casos, simplemente poco práctico. Mientras definimos los estándares de redes del futuro, Cisco está incorporando los últimos avances en IT a los equipos de redes industriales de hoy. Nuestros *switches* y routers industriales incorporan capacidades avanzadas de ciberseguridad que permiten obtener visibilidad a escala, facilitar microsegmentación para crear zonas industriales seguras y hacer que el acceso a la red de confianza cero funcione con las limitaciones específicas de las operaciones industriales. ●

Álvaro Fraile, director global de Servicios de Ciberseguridad de Ayesa



1. La ciberseguridad IT se orienta a proteger la confidencialidad, integridad y disponibilidad de la información en sistemas empresariales, como redes y bases de datos. En contraste, la ciberseguridad OT se enfoca en garantizar la seguridad y disponibilidad de sistemas que controlan procesos físicos en entornos industriales, donde la estabilidad operativa es crítica. Con la creciente convergencia entre IT y OT, los sistemas de control industrial están cada

vez más expuestos a amenazas cibernéticas. Por ello, es esencial comprender las diferencias entre ambas

áreas para implementar estrategias de protección que aseguren la continuidad operativa y la seguridad en sectores industriales clave.

2. Los ciberdelincuentes están sofisticando sus métodos de ataque a infraestructuras críticas al aprovechar la convergencia entre tecnologías de la información (IT) y tecnologías operativas (OT). Utilizan técnicas avanzadas como *ransomware*, dirigido, ataques de día cero y explotación de vulnerabilidades en sistemas *legacy*, combinados con ingeniería social para obtener acceso inicial. Además, se apoyan en la inteligencia artificial y el *machine learning* para automatizar y personalizar ataques, lo que aumenta su efectividad y la dificultad de detección. Esta evolución subraya la necesidad de una ciberseguridad ro-



—>

busta y adaptativa en entornos industriales para mitigar estos riesgos crecientes.

3. El factor humano desempeña un papel fundamental en la ciberseguridad industrial, ya que los trabajadores pueden ser tanto el eslabón más fuerte como el más débil en la defensa contra ciberamenazas. Errores humanos, como el clic en un enlace de *phishing* o la mala configuración de un sistema, pueden comprometer incluso las infraestructuras más seguras. Para mitigar estos riesgos, es crucial concienciar y formar a los empleados, transformándolos en la primera línea de defensa. Esto se logra mediante programas de capacitación continua que incluyan simulaciones de ciberataques, talleres prácticos y la implementación de políticas claras y accesibles de seguridad. Además, es vital fomentar una cultura organizacional de ciberseguridad, donde los trabajadores entiendan la importancia de su rol y las consecuencias potenciales de sus acciones. De esta manera, se fortalecen las defensas industriales y se aumenta la resiliencia ante posibles ciberataques.

4. La responsabilidad en la ciberseguridad industrial no recae en un solo actor, sino que es una responsabilidad compartida entre usuarios, integradores, proveedores de tecnología y gobiernos. Cada uno de estos grupos desempeña un rol esencial en la protección

de las infraestructuras críticas. Los usuarios, como operadores de los sistemas, son responsables de aplicar buenas prácticas de seguridad, mantener las operaciones seguras y estar en alerta ante posibles amenazas. Los integradores, quienes diseñan y configuran los sistemas industriales, deben garantizar que estos estén contruidos con seguridad desde el principio, minimizando las vulnerabilidades. Los proveedores de tecnología tienen la tarea de desarrollar productos resistentes a ciberataques y ofrecer actualizaciones regulares para abordar nuevas amenazas. Finalmente, los gobiernos han de establecer regulaciones claras, promover la creación de marcos de colaboración y facilitar la comunicación entre las diferentes partes. Fomentar una colaboración efectiva entre todos estos actores es fundamental para crear un ecosistema industrial más seguro. Esto se puede lograr a través de la creación de alianzas público-privadas, donde se comparta información sobre ciberamenazas en tiempo real, se desarrollen estándares de seguridad comunes y se organicen ejercicios de simulación de ciberataques. Además, es esencial la participación activa en iniciativas conjuntas de ciberseguridad, como grupos de trabajo sectoriales o foros de intercambio de información. Solo mediante una colaboración estrecha y continua se podrá enfrentar de manera efectiva el complejo panorama de amenazas que enfrenta la industria hoy en día. ●

Hugo Llanos, director del área de Ciberseguridad Industrial de Secure&IT (filial del Grupo LKS Next enfocada a ciberseguridad)

1. Si echamos la vista unos años atrás, no se planteaba la necesidad de implementar ciberseguridad en los entornos industriales. Esto se debía, principalmente, a la estanqueidad de las propias instalaciones, derivada de los medios propietarios empleados en la transmisión de la información y a la falta de necesidad de interoperar con otras instalaciones industriales o con sistemas enclavados en entornos IT. Era lo que se podría definir como un escenario de dos islas no comunicadas: IT y OT. Sin embargo, coincidiendo con la orientación mayoritaria de los fabricantes de soluciones de automatización industrial en el reemplazo de los medios físicos de comunicación entre componentes por otros basados en tecnología Ethernet, se facilitó el desarrollo y la puesta en marcha de un amplio abanico de aplicaciones que, partiendo de la posibilidad de acceder a las instalaciones industriales, mejoran de forma notable la operación de los procesos industriales y permiten obtener información operacional para optimizar el propio funcionamiento de los procesos de fabricación.

El entorno IT ya ha dado grandes pasos en la implementación de ciberseguridad. Podríamos decir que, salvo excepciones, la ciberseguridad se considera desde el diseño (y aun así ocurren ciberincidentes de forma habitual). Sin embargo, no ocurre lo mismo en el entorno OT, donde el “cambio”, o puesta en marcha a entornos de conectividad industrial requeridos por el negocio, se ha realizado sin la aplicación de las medidas de ciberseguridad adecuadas.

2. No cabe duda de que la vía principal de acceso a las instalaciones industriales sigue siendo a través del entorno IT, y los ataques a los sistemas (SCADA, MES, etc.) se basan principalmente en *malware* asociado típicamente a IT (*ransomware*, etc.) y no en ataques específicos a componentes de automatización que no estén basados en sistemas operativos de propósito general.



—>



Es cuestión de tiempo que, dentro de las tácticas de reconocimiento realizadas por los grupos atacantes se incluyan de forma habitual aquellas orientadas a la caracterización de redes industriales, que permitan la explotación de cualquiera de las múltiples vulnerabilidades que diariamente se identifican en componentes operacionales puros. A lo largo de los últimos años ya se han producido incidentes de este tipo, aunque generalmente ligados a ataques dirigidos.

3. El personal de planta es vital para la continuidad de la producción. Si le instruimos en cómo operar de forma segura (*safety*, seguridad física) una máquina, ¿por qué no le incluimos en los planes de concienciación en materia de ciberseguridad (*security*, seguridad lógica) que precisamente disminuyen la posibilidad de que se produzca un ciberincidente en los sistemas productivos?

Pensamos que el hecho de que un operario no disponga de credenciales de acceso a los sistemas corporativos no le excluye automáticamente de ser “usado” por un atacante para llegar hasta los sistemas industriales, obviando vectores de ataque como el uso de *pendrives*, el riesgo de conexiones de equipamiento de terceros a redes de planta, o las consecuencias de un mal uso del equipamiento informático corporativo, entre otros.

Animamos a las empresas a que, al igual que de forma frecuente disponen de paneles informativos con el número de accidentes y bajas que se han producido en un determinado periodo de tiempo, y que causan un efecto positivo en la prevención, se incorporen los datos relacionados con los ciberincidentes para lograr el mismo efecto.



Advanced SOC-CERT Secure&View está dotado de sistemas y procesos avanzados y es capaz de monitorizar, vigilar, registrar, gestionar y actuar de manera inmediata ante cualquier evento que afecte a la seguridad de la información de las organizaciones.

4. La principal responsabilidad recae en la alta dirección de las empresas que, por otro lado, generalmente no es consciente del nivel de riesgo en materia de ciberseguridad al que está expuesto el entorno industrial (y, por lo tanto, la continuidad del propio negocio). Establecer un sistema de gestión de la ciberseguridad industrial, incorporándola como un proceso corporativo más impulsado directamente por la dirección, es fundamental.

No hay que olvidar la necesidad de que nuestros proveedores incorporen la ciberseguridad desde el diseño. En este sentido, exigir medidas de seguridad desde el momento de la solicitud de ofertas nos permitirá evitar problemas a posteriori. ●

Gestión eficiente de la conectividad, clave del éxito para la digitalización

En la primavera de 2018, Cables RCT dentro del proceso de mejora continua y revisión de sus sistemas de ciberseguridad, realiza un análisis de los riesgos, detectando una oportunidad de mejora en su infraestructura de conectividad a su red OT. Conscientes de este potencial de mejora y a través de Araelec, su partner de confianza en soluciones industriales, contactaron con Siemens para buscar una solución que proporcionase, por un lado, una integración rápida y sencilla de las máquinas existentes en la infraestructura de conectividad y, por otro lado, que segmentase la red de manera adecuada, proporcionando un acceso remoto seguro a todas las máquinas. [Fragmento del artículo que José Luis Doñoro, responsable de Negocio de Conectividad Digital en Siemens Digital Industries España, y Juan Carlos Pozas Bustos, responsable de Ciberseguridad Horizontal en Siemens Digital Industries España, firman en las páginas 48 a 51].



Enrique Domínguez, responsable de CyberPhysical de Innotec Security, parte de Accenture

1. Mientras que la ciberseguridad IT se enfoca en la protección de la información, la privacidad de los datos y la continuidad de los servicios de TI, la ciberseguridad OT está más orientada a la disponibilidad, la seguridad física y la integridad de los sistemas de control industrial.

Hay una diferencia en los objetivos: en el ámbito IT, la confidencialidad de la información es primordial; en OT, la prioridad es mantener la continuidad y seguridad de las operaciones. La caída de un sistema IT puede significar pérdida de datos o tiempo de inactividad, mientras que en OT puede generar interrupciones en la producción, riesgos para la seguridad humana e incluso daños al medioambiente.

Una segunda diferencia en las prioridades: en IT, la protección contra *malware* y la prevención de fugas de información son fundamentales. Sin embargo, en OT, la preocupación principal es garantizar que los sistemas de control industrial operen sin interrupciones, lo que implica protegerlos de ataques que podrían manipular procesos físicos o interrumpir operaciones críticas.

Por último, una tercera diferencia en los entornos en los que operan: los sistemas IT suelen operar en entornos más estandarizados y actualizables, mientras que los sistemas OT son más heterogéneos y a menudo incluyen equipos y tecnologías que han estado en funcionamiento durante décadas. Estos sistemas suelen ser más difíciles de actualizar debido a su criticidad y, a veces, a la falta de soporte de los fabricantes.

Conocer estas diferencias es clave para proteger los sistemas de control industrial porque aplicar enfoques de ciberseguridad IT tradicionales a entornos OT sin adaptarlos puede ser ineficaz o incluso perjudicial. Es necesario un enfoque específico que considere la naturaleza crítica y sensible de los sistemas OT, donde un fallo puede tener consecuencias catastróficas, tanto en términos de seguridad física como de impacto económico.

2. Los ciberdelincuentes están sofisticando constantemente sus métodos de ataque adaptándose y aprovechando las vulnerabilidades emergentes en los sistemas de control industrial (ICS). Esta evolución se caracteriza por varios factores clave:

- Ataques dirigidos y personalizados: los atacantes están pasando de ataques masivos e indiscriminados a tácticas más dirigidas, específicamente diseñadas para vulnerar sistemas OT. Utilizan técnicas de *spear phishing*, ingeniería social y *zero-day* para infiltrarse en redes industriales con el objetivo de maximizar el



impacto.

- Uso de *malware* específico: han surgido varias familias de *malware* diseñadas específicamente para entornos OT, como Stuxnet, Triton y más recientemente, Industroyer2 o CosmicEnergy. Estos *malware* no solo buscan penetrar en los sistemas, sino también manipular procesos industriales críticos para causar daño físico o sabotear la producción.
- Exfiltración y secuestro de datos:

aunque la manipulación física de sistemas sigue siendo un objetivo, cada vez más ciberdelincuentes se centran en la exfiltración de datos sensibles y en el secuestro de información crítica mediante *ransomware*. Este tipo de ataques no solo comprometen la operación, sino que también buscan extorsionar a las organizaciones

- Explotación de la convergencia IT/OT: como ya hemos mencionado, a medida que las redes IT y OT convergen, los atacantes aprovechan esta integración para acceder a sistemas OT a través de vulnerabilidades en la infraestructura IT. Este enfoque multiplica las superficies de ataque y facilita la intrusión en entornos que antes estaban aislados o menos conectados.

- Amenazas internas: los ciberdelincuentes también están reclutando o coaccionando a empleados internos, quienes pueden tener acceso directo a sistemas críticos.

3. El factor humano juega un papel crucial en la ciberseguridad industrial, siendo tanto una de las mayores vulnerabilidades como una de las mejores defensas contra las ciberamenazas. Los trabajadores que operan y mantienen los sistemas de control industrial (ICS) son esenciales para proteger estas infraestructuras, pero también pueden ser, sin quererlo, vectores de acceso para los ciberdelincuentes. Los errores humanos, como la configuración incorrecta de sistemas, el uso de contraseñas débiles o la apertura de correos electrónicos de *phishing*, son puertas de entrada comunes para los atacantes. Además, la falta de familiaridad con las amenazas cibernéticas y con las prácticas de seguridad digital puede llevar a que los empleados no detecten señales de un ataque inminente.

Para que los trabajadores se conviertan en una barrera efectiva contra las ciberamenazas, es importante que comprendan las posibles amenazas y cómo prevenirlas. Esto se logra a través de programas de concienciación que expliquen, en términos claros y prácticos, cómo las amenazas cibernéticas pueden afectar su entorno de trabajo y cuáles son las mejores prácticas para



Accenture ofrece un enfoque integral para proteger infraestructuras y tecnologías industriales, desde la estrategia hasta la operación del SOC OT. Accenture cuenta con una práctica global en ciberseguridad OT con más de 22.000 personas a nivel global.

evitarlas. No basta con una formación inicial; el entorno de las ciberamenazas está en constante evolución. Las organizaciones deben implementar programas de formación continua que incluyan simulaciones de ataques, ejercicios de respuesta a incidentes y actualizaciones regulares sobre nuevas amenazas. Además, es necesario fomentar una cultura de seguridad en toda la organización. Esto implica que todos, desde la alta dirección hasta los operadores de planta, entiendan su responsabilidad en la protección de los sistemas. La seguridad debe ser vista como parte integral del trabajo diario, no como una obligación adicional.

Por último, los trabajadores deben sentir que cuentan con el apoyo adecuado para reportar incidentes o vulnerabilidades sin temor a represalias. La colaboración entre los equipos de IT y OT también es esencial para abordar las amenazas de manera holística.

4. La ciberseguridad industrial es una responsabilidad compartida que recae en todos los actores involucrados, por lo que la colaboración entre todos es esencial: usuarios y operadores, integradores, proveedores de tecnología y gobiernos. Cada uno de estos actores juega un papel crucial y complementario en la creación de un ecosistema industrial más seguro. Algunas formas de fomentar esta cooperación son las siguientes:

- Establecer plataformas y foros donde los diferentes actores puedan compartir información sobre amenazas, vulnerabilidades y mejores prácticas de forma proactiva y continua para adelantarse a las amenazas emergentes.
 - Los gobiernos pueden facilitar la creación de alianzas entre el sector privado y las agencias públicas para mejorar la respuesta a incidentes y el intercambio de información crítica.
 - Desarrollar y adoptar estándares de ciberseguridad que sean reconocidos globalmente, y establecer programas de certificación para asegurar que los productos y servicios cumplan con estos estándares.
 - Responsabilidad conjunta en la gestión de incidentes. Crear protocolos de respuesta a incidentes que involucren a todos los actores relevantes, asegurando que, en caso de un ataque, haya una respuesta coordinada y efectiva para minimizar el impacto.
- Al fomentar la colaboración, compartir conocimientos y establecer estándares comunes se puede construir un ecosistema industrial resiliente y capaz de enfrentar las amenazas cibernéticas del futuro. ●

David Ruiz Estepa, Cybersecurity Technical Leader de Mytra

1. Las diferencias clave entre la ciberseguridad IT y OT radican en sus enfoques y prioridades. En IT, la ciberseguridad se centra en proteger los datos y los sistemas para garantizar la confidencialidad, integridad y disponibilidad de la información. En cambio, en OT, la principal preocupación es asegurar la continuidad y seguridad de los procesos industriales, donde la disponibilidad es crucial, ya que cualquier tiempo de



inactividad puede tener graves consecuencias económicas y operativas. A la hora de proteger los sistemas de control industrial (ICS), es importante tener en cuenta dos factores que los diferencian de los entornos IT. Primero, los entornos OT emplean una amplia variedad de tecnologías y protocolos específicos de la industria, lo que puede introducir más vulnerabilidades en comparación con los entornos IT, que sue-



—>

len utilizar tecnologías más estandarizadas. Segundo, la implementación de actualizaciones o soluciones de seguridad en OT puede ser más compleja, ya que a menudo requiere interrumpir las operaciones, algo que no siempre es viable sin afectar la producción. Es importante entender estas diferencias para diseñar estrategias de ciberseguridad que se adapten a las necesidades específicas de los sistemas industriales. Implementar estrategias de ciberseguridad IT directamente en entornos OT puede ser ineficaz o incluso contraproducente.

2. El incremento en la conectividad ha elevado el riesgo de ciberataques. Los atacantes están cada vez más sofisticados en sus métodos, explotando vulnerabilidades en dispositivos conectados para acceder a redes OT y lanzar ataques específicos a sistemas de control industrial. Estos tipos de *malware* no solo comprometen datos, sino que también manipulan procesos físicos y pueden interrumpir operaciones críticas, lo que subraya la necesidad de medidas de seguridad avanzadas y específicas para entornos industriales. Por otro lado, los ataques a la cadena de suministro se han convertido en una estrategia clave para los ciberdelincuentes.

A través de proveedores o terceros que tienen acceso a sistemas críticos, los atacantes logran introducirse en infraestructuras sensibles. Por esta razón, es esencial mantener una vigilancia constante y colaborar estrechamente con proveedores y socios para asegurarse de que las defensas de ciberseguridad sean robustas, estén actualizadas y puedan contrarrestar las amenazas emergentes de manera eficaz.

3. El factor humano es la primera barrera frente a los ciberataques. Acciones como hacer clic en enlaces sospechosos, reutilizar contraseñas o compartir información sin tomar precauciones pueden abrir la puerta a ataques que pueden comprometer a los sistemas críticos. Además, los riesgos no solo provienen de errores involuntarios; también existen amenazas internas cuando los empleados actúan con negligencia o intenciones maliciosas.

Para fortalecer esta primera línea de defensa, es indispensable crear una cultura organizacional donde la ciberseguridad sea una responsabilidad compartida. Esto implica implementar políticas claras y procedimientos accesibles, así como desarrollar programas de concienciación y formación continua que capaciten a los empleados en buenas prácticas de ciberseguridad.

Estos programas deben enfocarse en ayudar a los empleados a reconocer y responder a amenazas comunes como el *phishing* o el manejo seguro de datos sensibles. Las simulaciones de ciberataques y los ejercicios prácticos son herramientas efectivas para preparar a los trabajadores ante incidentes reales.



Mytra ofrece servicios de consultoría e integración de soluciones basadas en las mejores prácticas de los estándares y normativas (IEC 62443, NIS2 y ENS), adaptadas a las necesidades de cada cliente.

4. Debido a la complejidad de las infraestructuras críticas y la diversidad de amenazas, la ciberseguridad industrial es una responsabilidad compartida entre usuarios, integradores, proveedores de tecnología y gobiernos. Cada uno de estos actores es fundamental para garantizar la disponibilidad, integridad y confidencialidad en los entornos OT. Los proveedores de tecnología deben desarrollar soluciones bajo principios de seguridad por diseño, cumpliendo con estándares avanzados de ciberseguridad.

Los integradores son responsables de la correcta implementación de estas tecnologías, asegurando configuraciones seguras y adaptadas a los requisitos operativos. Los usuarios deben adoptar políticas de seguridad rigurosas, mantener la infraestructura actualizada y aplicar procedimientos de respuesta a incidentes. Por su parte, los gobiernos tienen que establecer marcos regulatorios robustos que promuevan la cooperación y la resiliencia en infraestructuras críticas. La creación de un ecosistema de ciberseguridad industrial robusto exige una colaboración continua entre todos estos actores. Esto implica compartir información sobre amenazas, llevar a cabo iniciativas conjuntas de seguridad y desarrollar buenas prácticas operativas, apoyadas en normativas específicas del sector como el estándar ISA/IEC 62443. ●

David Marco Freire, director de Ciberseguridad Industrial/OT en KPMG



1. La ciberseguridad IT se centra en la protección de datos e información, con un enfoque en la prevención de acceso no autorizado y la protección de la confidencialidad de los datos. Las actualizaciones de seguridad en IT se aplican rápidamente para mitigar vulnerabilidades y las redes suelen ser abiertas, con un fuerte énfasis en la seguridad de la red. Los usuarios principales de IT son el personal de oficina y los equipos de TI.

Por otro lado, la ciberseguridad OT se enfoca en garantizar la disponibilidad y seguridad de los procesos físicos. Su principal objetivo es la resiliencia y la continuidad operativa de los sistemas de control industrial. Las actualizaciones de seguridad en OT se aplican con cuidado para evitar interrupciones en los procesos críticos, y las redes suelen ser cerradas y aisladas. Los usuarios de OT son principalmente ingenieros y personal de planta.

Entender estas diferencias es crucial para proteger los sistemas de control industrial, ya que los enfoques de seguridad deben adaptarse a las necesidades específicas de cada entorno. La ciberseguridad OT se centra en la continuidad operativa y la integridad de los procesos industriales, mientras que la ciberseguridad IT prioriza la protección de datos. Una estrategia de seguridad efectiva debe integrar ambos enfoques para asegurar una protección integral.

2. Los ciberdelincuentes están adaptando sus métodos de ataque a infraestructuras críticas de manera sofisticada y técnica. Algunas de las técnicas que están utilizando son:

- El uso de *malware* sofisticado, como variantes de Stuxnet, permite evadir detección y persistir en sistemas críticos, causando daños significativos.
- Los ataques de ransomware ahora incluyen cifrado de datos, exfiltración de información sensible y amenazas de ataques DDoS si no se paga el rescate.
- El uso de vulnerabilidades de día cero permite a los atacantes infiltrarse en sistemas antes de que se apliquen parches de seguridad, explotando fallos desconocidos.
- Comprometer proveedores de software o hardware para infiltrarse en las redes de sus clientes, como el ataque a SolarWinds, se ha vuelto más común.
- Los ciberdelincuentes aprovechan configuraciones incorrectas y vulnerabilidades en servicios en la nube para lanzar ataques DDoS o alojar *malware*.
- Los ataques de *phishing* y *spear phishing* dirigidos a empleados de infraestructuras críticas siguen siendo efectivos para obtener acceso inicial a redes internas.
- El uso de inteligencia artificial y aprendizaje automático permite automatizar ataques y mejorar la eficacia de los métodos de ciberataque.

Estas tendencias subrayan la necesidad de medidas de seguridad avanzadas y vigilancia constante para proteger infraestructuras críticas.

3. El factor humano es crucial en la ciberseguridad industrial, ya que los empleados pueden ser tanto una defensa esencial como una vulnerabilidad. Los errores humanos, como contraseñas débiles o la apertura de correos de *phishing*, son responsables de muchas brechas de seguridad. Además, los ataques de ingeniería social dependen de la manipulación del comportamiento humano. Para que los trabajadores tengan conciencia de ciberseguridad podemos desarrollar estas prácticas:

- Formación continua: implementar programas de formación actualizados regularmente sobre las últimas amenazas y técnicas de ataque.
 - Simulaciones de ataques: realizar ejercicios de *phishing* y otros ataques para que los empleados aprendan a reconocer y responder adecuadamente.
 - Cultura de seguridad: promover la importancia de la ciberseguridad desde la alta dirección y asegurar que todos comprendan su papel en la protección de la empresa.
 - Políticas claras: establecer y comunicar políticas sobre el uso de sistemas y datos.
 - Tecnología de apoyo: utilizar autenticación multifactor y gestión de identidades para reducir errores humanos.
 - Educación en ingeniería social: enseñar a los empleados a identificar y evitar tácticas de ingeniería social.
- Estas estrategias ayudan a fortalecer la primera línea de defensa contra las ciberamenazas.

4. La responsabilidad en la ciberseguridad industrial es compartida entre usuarios, integradores, proveedores de tecnología y gobiernos:

- Deben seguir políticas de seguridad y reportar actividades sospechosas. La formación continua es esencial.
- Aseguran que las soluciones cumplan con los estándares de seguridad y sean resistentes a ciberataques.
- Desarrollan productos seguros, aplican parches regularmente y ofrecen soporte continuo.
- Establecen regulaciones y estándares, fomentan la colaboración público-privada y proporcionan recursos para la investigación y respuesta a incidentes.

1. Foros y alianzas: plataformas para compartir información y mejores prácticas.

2. Programas de concienciación: campañas educativas sobre ciberseguridad.

3. Normativas comunes: regulaciones que aseguren un nivel mínimo de seguridad.

4. Investigación conjunta: proyectos colaborativos para desarrollar nuevas tecnologías y estrategias de defensa.

Una colaboración efectiva es esencial para un ecosistema industrial seguro y resiliente. ●

Agustín Valencia, OT Security Business Development Manager Iberia en Fortinet

1. De acuerdo con la definición de una reconocida firma de análisis “OT son prácticas y tecnologías que se utilizan para proteger personas, activos e información, monitorizar o controlar dispositivos físicos, procesos y eventos, e iniciar cambios de estado en los sistemas de OT empresariales”. Como su propio nombre indica, OT son tecnologías centradas en la “operación”, es decir, involucradas directamente con los procesos operativos de la empresa. Por su parte, las tecnologías de la información (TI) ponen el foco en la información. En resumen, la tecnología operativa se enfoca a procesos con controles y protecciones en tiempo real, mientras que la tecnología de la información (TI) gestiona solamente datos.

Si nos centramos en sus principales diferencias, que son múltiples, cabría destacar que el impacto en la sociedad ante el fallo de tecnologías OT es mucho más sensible y puede conllevar fallos en cascada.

Además, el entorno OT se caracteriza por su dispersión geográfica y su localización compleja en zonas incluso de difícil acceso, lo que requiere que los equipos responsables de sus sistemas trabajen en condiciones complicadas. Imaginemos, por ejemplo, un aerogenerador en lo alto de una montaña o una fábrica a miles de kilómetros de los servicios centrales. Por otro lado, los dispositivos que forman parte de los entornos OT (instrumentos, motores, controladores, protecciones...) son muy variados y con muchos fabricantes específicos de cada sector de actividad, con lo que supone en heterogeneidad para la gestión del parque de activos y de la cadena de suministro. Por último, al tratarse de industrias críticas para la sociedad, los entornos OT cuentan con una regulación muy estricta y específica.

Teniendo en cuenta que la convergencia TI-OT es un hecho que sigue avanzando, es imprescindible conocer las particularidades de los entornos OT para protegerlas frente a las amenazas y vulnerabilidades conocidas en TI que también les pueden afectar.

2. El reciente Informe global sobre el Estado de la Tecnología Operativa y la Ciberseguridad 2024 de Fortinet confirma que sigue habiendo muchos puntos ciegos en su entorno. Los datos del informe reflejan que, desde el pasado año, ha disminuido el porcentaje de organizaciones que afirmaban tener una visibilidad completa de los sistemas OT dentro de sus operaciones centrales de seguridad, pasando del 10% al 5%. Sin embargo, los que afirman tener un 75% de visibilidad han aumentado, lo que sugiere que las organizaciones están adquiriendo un conocimiento más realista de su postura de seguridad.

Las intrusiones de ransomware o wiper siguen aumentando, de hecho, más de la mitad (56%) de los encuestados confirmaron haber sufrido estos ataques, por lo que hay margen de mejora en relación con la visibilidad de la red y las capacidades de detección.

3. El factor humano es determinante para frenar las ciberamenazas y así lo corroboramos en el último informe que realizamos sobre la brecha de competencias en ciberseguridad de Fortinet en el que se reveló que cada vez más las organizaciones atribuyen las brechas de seguridad a la falta de competencias en esta materia. Para el 30% de las organizaciones encuestadas en EMEA, la inteligencia sobre ciberamenazas es la competencia más necesaria, si bien en el caso de España solo el 18% de las mismas la señalaron como la más importante.

Para hacer frente a esta problemática, las organizaciones están adoptando un triple enfoque de la ciberseguridad que combina formación, concienciación y tecnología. Conscientes de esta necesidad de formación, en Fortinet nos hemos marcado como objetivo formar a un millón de personas en ciberseguridad para 2026 y ya nos estamos acercando al medio millón.

4. La responsabilidad no recae en un solo actor, sino que es una responsabilidad compartida que no cae únicamente en el responsable de ciberseguridad o el CISO. De hecho, la regulación NIS2 avanza en apuntar hacia el negocio y el comité de dirección como responsables últimos, el peso del negocio en el éxito de las iniciativas de ciberseguridad es absolutamente decisivo en la ciberseguridad industrial. Por otro lado, esta misma regulación apunta a la seguridad de la cadena de suministro, lo que supone un gran reto para los usuarios finales. Fortinet es uno de los primeros proveedores de ciberseguridad que ha firmado el compromiso Secure by Design de CISA, lo que confirma nuestro compromiso a una cultura de transparencia integral responsable con la seguridad de nuestros clientes. La colaboración con todo el ecosistema, tanto asociaciones públicas como privadas, ha sido siempre una de nuestras prioridades. Somos miembro fundador de la Network Resilience Coalition y de la Cyber Threat Alliance (CTA), pertenecemos a la Joint Cyber Defense Collaborative (JCDC), y colaboramos con otras entidades líderes a nivel mundial como miembros fundadores del Centro para la Ciberseguridad (C4C) del Foro Económico Mundial. ●



Pedro Castro Requejo, coordinador del área de Digitalización de Grupo Iturcemi



1. La principal diferencia se basa en la disponibilidad de la información, siendo prioritaria en OT, mientras que en IT el foco se centra en la confidencialidad de la información. El fijar el foco en la disponibilidad suele ser el principal obstáculo que se encuentran los profesionales que desde IT afrontan proyectos orientados a OT, ya que, por ejemplo, un sistema industrial no puede ser detenido “aleatoriamente” para carga de actualizaciones, las comunicaciones en redes industriales deben estar limitadas a las propias del proceso, por lo que es necesario una segmentación profunda o las gestiones de accesos deben ser tratadas con diferentes perspectivas debido a la criticidad de los sistemas, evitando por ejemplo los cierres automáticos de sesión o la caducidad de contraseñas en usuarios de servicios.

2. La hiperconectividad que está inundando el mundo industrial abre la puerta a nuevos vectores de ataque que antes no existían. Tradicionalmente, el principal riesgo en las instalaciones industriales venía por la intervención humana, bien debido a fallos en el manejo de sistemas, bien debido a sabotajes u operaciones malintencionadas. Hoy en día, los sistemas de la capa de operación están altamente relacionados con los sistemas de la capa de información, e incluso con conexiones a ubicaciones en la nube, lo que abre la puerta a una gran variedad de ataques que anteriormente se focalizaban en la capa de información. El cifrado y secuestro de equipos de supervisión o la corrupción de la información enviada a los sistemas de control provoca paradas en los sistemas de operación que pueden conllevar pérdidas millonarias a las compañías,

por lo que es fundamental volcar esfuerzos en la protección de los activos, con estrategias básicas como la segmentación de zonas y conductos.

3. Sin duda alguna, el factor humano es clave a la hora de afrontar cualquier programa de ciberseguridad industrial. En muchas ocasiones, las medidas de ciberseguridad a implementar pueden conllevar modificaciones en metodologías de trabajo y es necesario la implicación absoluta de todo el personal de la instalación. Es necesario programas planes de concienciación para que toda la plantilla de una instalación vaya asumiendo la importancia de la ciberseguridad para el negocio y entendiendo que ya no es un asunto exclusivo de informáticos, sino que es un concepto de ámbito global, de la misma manera que la seguridad laboral. Un incidente de ciberseguridad industrial puede ocasionar no solo pérdidas económicas, como en el caso de la capa de información, sino que puede generar incidentes mucho más graves afectando a la salud de las personas.

4. La responsabilidad en la ciberseguridad industrial es coral, todos los actores participantes en el sistema tienen su cuota de responsabilidad y deben implicarse en el cumplimiento y promoción de las políticas de ciberseguridad. Los gobiernos tienen que fijar regulaciones y fomentar normativas que sean adaptables de manera razonable en el tiempo, y que no supongan inversiones desproporcionadas respecto al tamaño de la empresa. La dirección de las empresas ha de involucrarse al diseñar e implementar programas de ciberseguridad, dedicando los recursos humanos y económicos necesarios. Por último los trabajadores deben tener muy presente las políticas diseñadas y esmerarse en su cumplimiento. Para conseguir que todos los actores colaboren en obtener resultados, la concienciación es fundamental. El ejemplo con el que hay que compararse es la seguridad laboral, como hace 20 años el uso de EPIs obligatorios era casi anecdótico en muchas empresas, y hoy en día es impensable acceder a un centro de producción sin las medidas de protección adecuadas. En esa línea es en la que se debe avanzar, de manera que la ciberseguridad este integrada en las primeras fases de diseño de las soluciones productivas, sea fomentada por la dirección, no solo por el cumplimiento de regulaciones, sino como propia política empresarial, y aceptada y aplaudida por los trabajadores, reconociendo un puesto de trabajo mucho más seguro y estable. ●

Adriel Regueira Suárez , Senior Sales Engineer en Nozomi Networks



1. La ciberseguridad, aunque comparte los mismos conceptos tanto en el entorno corporativo (IT) como en el industrial (OT), es diferente en su aplicación y en los objetivos que se buscan proteger. En los entornos corporativos, el principal enfoque es mantener la confidencialidad de los datos y la integridad de los mismos, mientras que en los sistemas industriales, la prioridad recae sobre la disponibilidad. En este contexto, asegurar que los sistemas continúen operando sin interrupciones es fundamental, ya que una paralización puede tener un impacto económico directo en la empresa afectada.

Aunque esta diferencia es generalmente aceptada, hay matices importantes según la industria. Por ejemplo, en el sector farmacéutico, además de garantizar la continuidad operativa, es crucial proteger la confidencialidad de las fórmulas y recetas, y evitar manipulaciones que podrían generar productos dañinos para la salud. En la industria alimentaria o en la gestión de recursos como el agua, cualquier alteración de los parámetros controlados podría tener consecuencias graves para los consumidores, llegando incluso a poner en peligro la vida de las personas. En el ámbito IT, los sistemas suelen ser fácilmente parcheables y mantenidos al día, lo que reduce las vulnerabilidades. Además, se pueden implementar soluciones de seguridad como antivirus (EDR, XDR) que refuerzan la protección. Sin embargo, en los entornos industriales, los equipos como los PLCs y HMIs son mucho más antiguos y fueron diseñados sin tener en cuenta la ciberseguridad. Estos dispositivos suelen operar con protocolos no autenticados y sin cifrado, lo que los hace todavía más vulnerables. Además, son difíciles de parchear, ya que cualquier interrupción en su operación para actualizarlos puede ser muy costosa y disruptiva, y, muchas veces, con un coste difícilmente justificable.

Por ello, la ciberseguridad en entornos ciberfísicos no solo implica pérdidas económicas o de datos, sino que puede suponer un riesgo directo para la vida de las personas. Es vital comprender estas diferencias para proteger adecuadamente estos y detectar y mitigar los riesgos asociados.

2. Los ciberdelincuentes están aprovechando las vulnerabilidades de los sistemas ciberfísicos, que a menudo no fueron diseñados pensando en la ciberseguridad. Estas vulnerabilidades, cada vez más conocidas, permiten a los atacantes comprometer infraestructuras críticas con un gran impacto. Además, los ataques se han vuelto más sofisticados, utilizando ransomware, espionaje industrial y ataques promovidos por Estados. Los ciberdelincuentes también están aprovechando nuevas tecnologías como la inteligencia artificial para automatizar ataques.

Un enfoque al alza es atacar la cadena de suministro y los dispositivos IoT, ya que muchos no están bien protegidos y pueden ser un punto de entrada a redes más amplias y con más impacto. Las motivaciones han pasado de ser principalmente económicas a incluir el caos, la interrup-

ción de servicios esenciales o la influencia política. También es común que los ataques sean de larga duración y difíciles de detectar, permaneciendo en los sistemas antes de provocar daños mayores.

3. El factor humano, tanto en el ámbito corporativo como en el industrial, sigue siendo el principal vector por el que penetran los ciberataques. Siempre insisto en mis charlas que, a menudo, no hay mejor “hacker” que el propio operario de turno de noche que, por ejemplo, busca ver un partido en línea desde el equipo de la planta. Este tipo de acciones puede generar vulnerabilidades que los ciberdelincuentes pueden explotar fácilmente.

Es indispensable formar y concienciar a los trabajadores de la misma manera que se hace en prevención de riesgos laborales. Todos deben entender que sus acciones con los equipos disponibles en la empresa pueden suponer un riesgo. Cada herramienta y sistema tiene un propósito específico y aunque en el corto plazo algo pueda parecer beneficioso, es esencial considerar que toda acción conlleva un riesgo asociado. Por eso, los empleados deben estar informados sobre ello, ser conscientes de los mismo, y aprender a evaluar si el beneficio compensa el riesgo o preguntar a un responsable-decisor que sea quien lo evalúe.

Afortunadamente, en los últimos años, hemos avanzado mucho en España en cuanto a la concienciación sobre ciberseguridad. Anteriormente, el tema se veía como algo lejano, algo que “algún día habría que tratar”. Hoy, la mayoría de personas con las que hablo ya entienden que es un tema imprescindible. Muchos han sido víctimas de ciberataques o conocen a alguien que lo ha sido, ya sea por estafas, robo de datos o ataques de ransomware.

Aunque hemos mejorado en la toma de conciencia, es necesario continuar educando a las personas sobre los riesgos y cómo identificarlos. Debemos fomentar una cultura de precaución y reflexión, para que, ante cualquier actividad sospechosa (o no), los trabajadores se detengan a pensar en las posibles consecuencias antes de actuar.

4. La responsabilidad en la ciberseguridad industrial es compartida entre usuarios, integradores, proveedores de tecnología y gobiernos. Cada uno desempeña un papel crucial y el éxito en proteger las infraestructuras críticas depende de una colaboración efectiva entre todos. Los integradores, por su parte, no solo implementan soluciones, sino que también deben garantizar que cumplen con los más altos estándares de ciberseguridad. Al estar certificados y pasar auditorías rigurosas, pueden añadir valor a sus servicios, minimizando los riesgos que podrían introducir a las empresas a las que sirven. Igualmente, los proveedores de tecnología tienen la responsabilidad de desarrollar productos seguros desde su diseño, con protocolos actualizados que permitan a las



organizaciones enfrentar las amenazas emergentes. Los gobiernos, como en el caso de España con el Incibe, tienen la obligación de legislar y normativizar. La implementación de regulaciones como la directiva NIS II en Europa, y su adaptación en el país, está ayudando a concienciar a todos los actores sobre la importancia de poner

medios efectivos para mitigar los ciberriesgos. Una colaboración sólida es esencial. Crear espacios de intercambio de información y mejores prácticas entre sectores, junto con alianzas público-privadas, permitiría construir un ecosistema industrial más seguro y resiliente frente a las ciberamenazas. ●

Raúl Núñez, Sales Engineer Team Lead en Trend Micro Iberia



1. Cuando hablamos de seguridad en entornos industriales, tenemos que entender que es un entorno en el que prevalece la producción por encima de todo y que una mala práctica o aplicación de política de seguridad puede hacer perder millones o incluso afectar a vidas humanas. Si en una red IT ponemos una política de seguridad en la que

un usuario o grupo de usuarios dejan de navegar, no es algo del todo crítico, pero si se cortan las comunicaciones o la ejecución de un proceso en un entorno industrial puede tener repercusiones económicas millonarias.

2. En los últimos dos años se observa un cambio en la mentalidad de las empresas hacia este tipo de entornos debido a la criticidad de los mismos, y que nunca han sido pensados ni diseñados teniendo en cuenta la seguridad informática.

Se sabe que gran número de sistemas están desprotegidos, en muchos de los casos porque al ser redes aisladas, o supuestamente aisladas, se piensa que no es necesario proteger. La realidad es que las soluciones que se desplegaban para este tipo de entorno siempre habían sido soluciones pensadas en IT, y esto ha hecho que se descartasen las protecciones por el gran número de falsos positivos que puede llegar a dar una solución de IT en este tipo de entornos.

A día de hoy, gran número de empresas han empezado a abordar la protección de este tipo de entornos OT y sobre todo desde una primera fase inicial: la de descubrimiento, es decir, conocer el entorno en el que se ha de trabajar.

Antes de poner en marcha una política de seguridad es importante saber a qué nos enfrentamos:

- Qué sistemas operativos y versiones tenemos
- Qué aplicativos
- Qué tipos de dispositivos

Esto nos permite tener una primera fase para hacer un análisis de riesgo de nuestro entorno industrial y proceder a una toma de decisiones adecuada.

3. Hay que partir de la base de que tenemos que tener en cuenta que las personas que operan las redes industriales son personas que no han sido formadas en seguridad informática y su trabajo es velar por la producción de la empresa.

Es importante que se les informe debidamente de la importancia de los datos que están tratando, de cuán perjudicial puede ser usar un dispositivo de almacenamiento externo dentro de una red industrial y, lo más importante, no solo hay que formarles a ellos, sino que nosotros, como expertos en seguridad, tenemos que entender su trabajo día a día para adecuar la seguridad a su manera de trabajar. Esto es clave.

Se trata de una información bidireccional para que una política de seguridad tenga éxito en una red de producción OT.

4. Todos los que acceden o deben acceder a la red industrial deben tener la concienciación de seguridad. De nada vale que una empresa ponga todas las protecciones necesarias si llega un proveedor y no tiene la misma consideración con los datos o los accesos del cliente. Las redes industriales están categorizadas en base a un nivel de criticidad. Por ejemplo, una red de transportes es una red crítica, con lo cual, además de que los propios trabajadores y proveedores deben formar parte de la seguridad, el gobierno tiene que tomar la misma responsabilidad y concienciación. ¿Qué ocurriría si se recibe un ataque informático y se paralizan las redes de transporte o los suministros de agua y luz?

Sobre cómo se puede fomentar una colaboración efectiva entre todos los actores para crear un ecosistema industrial más seguro, hay que decir que la compartición de información y de experiencias es una de las acciones más efectivas, seguimos siendo demasiado reticentes a compartir nuestras “vergüenzas”, pero esto puede hacer que una empresa que ya se haya enfrentado a un problema de seguridad pueda habilitar a otra para prevenir o mejorar sus sistemas. ●



TXOne EdgeIPS
aporta transparencia
y tiene la habilidad
de segmentar activos,
mejorando así la
capacidad de defensa
de la red del lugar de
trabajo de una forma
importante.



**Salón Internacional de
Soluciones para la Industria
Eléctrica y Electrónica.**

05-08 2024
Nov

Recinto Ferial
ifema.es

Ciberseguridad y conectividad avanzada en la industria

GESTIÓN EFICIENTE DE LA CONECTIVIDAD, CLAVE DEL ÉXITO PARA LA DIGITALIZACIÓN

En la primavera de 2018, Cables RCT dentro del proceso de mejora continua y revisión de sus sistemas de ciberseguridad, realiza un análisis de los riesgos, detectando una oportunidad de mejora en su infraestructura de conectividad a su red OT. Conscientes de este potencial de mejora y a través de Araelec, su partner de confianza en soluciones industriales, contactaron con Siemens para buscar una solución que proporcionase, por un lado, una integración rápida y sencilla de las máquinas existentes en la infraestructura de conectividad y, por otro lado, que segmentase la red de manera adecuada, proporcionando un acceso remoto seguro a todas las máquinas.

■ **José Luis Doñoro**, Responsable de Negocio de Conectividad Digital en Siemens Digital Industries España

Juan Carlos Pozas Bustos, Responsable de Ciberseguridad Horizontal en Siemens Digital Industries España — 



Cables RCT es un fabricante español de cables eléctricos de baja tensión ubicado en Zaragoza desde 1965. Los valores

de la empresa son el compromiso a largo plazo, la seguridad y la confianza, y tiene como objetivo ser un proveedor de cables para la vida diaria y para diferentes industrias. Cables RCT ha decidido estratégicamente adaptar sus instalaciones, máquinas y procesos de producción para evolucionar con las nuevas tecnologías y cumplir con los cambios de legislación. A raíz de la situación mencionada anteriormente, nació un proyecto que tenía como objetivo crear una infraestructura de red industrial para proteger las instalaciones y las máquinas de Cables RCT, que ocupan un área de 30.000 metros cuadrados y que al final también ayudó a mantener la competitividad en el mercado.

Ángel Ventura, director de ingeniería en Cables RCT, destaca "Uno de los mayores desafíos que enfrentamos en el proyecto fue la segmentación de la red para garantizar la seguridad del acceso a las máquinas tanto internamente desde planta como desde el exterior. Teníamos que asegurarnos de que el sistema fuera fiable y que al mismo tiempo no hubiera interrupciones en el proceso productivo".

"Otro punto que es importante para nosotros es la continuidad a largo plazo del proyecto, ya que Siemens garantiza la disponibilidad de componentes para repuesto y para futuras ampliaciones en caso de ser necesario, lo que no siempre es posible con otros proveedores del mercado" explica Carlos Bazán, director técnico de Araelec.

Integración eficaz y duradera en automatización y gestión de redes industriales

Siemens, junto con el partner de Cables RCT, Araelec, especialista en soluciones industriales, realizó una propuesta destacando la implementación rápida y sencilla de la solución diseñada en las máquinas existentes con diferente antigüedad y de distintos proveedores, con una colaboración abierta y constante entre los equipos de IT y OT en Cables RCT. Al



Aquí podemos ver la clásica familia SCALANCE X200 conectada a través de SCALANCE SC600.

hablar desde Siemens el lenguaje de ambos mundos y facilitar la llegada a puntos de encuentro, resultó en una colaboración exitosa entre los dos grupos de trabajo que garantizó el éxito del proyecto en su totalidad. La integración segura de la infraestructura OT con la infraestructura de IT ha permitido a Cables RCT capturar y analizar los datos de producción de manera más eficiente para mejorar sus procesos. Además, la capacidad de Siemens para ofrecer soluciones de alto nivel y de implementación sencilla ha permitido modernizar las instalaciones sin interrumpir la producción. El enfoque centrado en la ciberseguridad de Siemens ha permi-

tido a Cables RCT mitigar los riesgos existentes y asegurar la continuidad de su producción.

Mejorando la seguridad y la fiabilidad con las soluciones integradas

Siemens, utilizando su amplio catálogo de productos y soluciones, ayudó a Cables RCT a superar sus desafíos de ciberseguridad y mejorar su infraestructura. Uno de los elementos clave en la solución fue la plataforma de gestión de conectividad SINEMA Remote Connect. "Este software, diseñado para la gestión de accesos remotos y la conectividad en planta, proporciona una solución segura y escalable que garantiza el acceso a las máquinas, miti-

Ventajas y beneficios para Cables RCT

- Mayor nivel de seguridad en el área OT.
- Ahorro de costes al reducir tiempos y eliminar desplazamientos en el servicio de máquinas.
- Mejora de los procesos y de la calidad de los productos.
- Asegurar la continuidad de la producción.
- Conectividad segura con todas las máquinas, incluso con las más antiguas.
- Estandarización de una solución escalable que permite ampliaciones futuras.
- Acceso inmediato a máquinas para personal de mantenimiento interno.
- Excelente colaboración entre los equipos de IT y de OT
- Digitalización de los procesos al tener conectividad total a las máquinas.



Es imprescindible disponer de acceso remoto seguro sin causar paradas en la producción. Angel Ventura, director de ingeniería junto con Javier Mallor responsable de automatización.

gando los riesgos de ciberseguridad” destaca Edgar Romeo, director de tecnologías de la información en Cables RCT. “Este sistema permite la gestión segura y eficiente de las conexiones, independientemente de su ubicación, haciendo posible la monitorización y el servicio a distancia de la planta.”

Para mejorar la gestión de la red y la comunicación entre diferentes dispositivos, se utilizaron los switches industriales SCALANCE XC216-4C y SCALANCE XC208. Estos switches gestionables son muy importantes para el flujo de los datos dentro de la infraestructura de la planta. El

SCALANCE XC216-4C SFP, un switch industrial con conexiones de fibra óptica a Gigabit Ethernet, proporciona alta velocidad y rendimiento, lo que facilita una transmisión de datos eficiente en el anillo de backbone industrial. Por otro lado, el SCALANCE XC208, un switch industrial con conexiones de cobre Fast Ethernet, garantiza una comunicación estable y fiable entre los dispositivos de la propia máquina, minimizando las interrupciones y maximizando la productividad. Además, se incluyó el SCALANCE SC636-2C en la solución. Este dispositivo es un router con funcionalidad de seguridad que añade una capa adicional de protección para la red de Cables RCT. Está diseñado para segmentar las células de automatización, en este caso las máquinas, a la vez que ofrece una comunicación segura gestionada desde la herramienta SINEMA Remote Connect. Este router es crucial para mantener la integridad de la red, y su inclusión en la solución proporcionó a Cables RCT una red más segura y fiable. Finalmente, para garantizar la alimentación eléctrica continua y fiable



El sistema productivo de Cables RCT cuenta con los equipos más actuales para la fabricación de cables eléctricos aislados para baja tensión. Cables RCT es un proveedor de cables para todos los días y cables para toda la vida.



Personal de mantenimiento de Cables RCT utilizando la herramienta SINEMA Remote Connect. Gracias a la solución integrada, ahora es posible el acceso seguro a las máquinas tanto desde el interior como desde el exterior de la fábrica.

a todos estos dispositivos, Siemens proporcionó la SITOP PSU100S, una fuente de alimentación industrial. Esta fuente de alimentación asegura que todos los dispositivos y máquinas en la planta estén siempre operativos y no sufran interrupciones debido a problemas de energía. De este modo, la SITOP PSU100S garantiza la continuidad operativa de la planta, contribuyendo a su eficiencia y productividad. Con todos estos productos formando una solución de conjunto, Siemens permitió que Cables RCT mejorara significativamente su infraestructura

de conectividad industrial en el área OT, respondiendo adecuadamente a sus necesidades.

Los resultados superan las expectativas

La ayuda de Siemens junto con Araelec en el proyecto para Cables RCT ha ido más allá de la consultoría técnica. “Durante el proceso de planificación y ejecución del proyecto, Siemens se ha convertido en un verdadero socio tecnológico para nosotros. Además de proporcionar soluciones técnicas de automatización de primer nivel, Siemens ha colaborado estrechamente con nosotros y Araelec

Lista de productos Siemens

- SINEMA Remote Connect.
- SCALANCE XC216-4C.
- SCALANCE XC208.
- SCALANCE SC636-2C.
- SITOP PSU100S.

para entender nuestras necesidades y metas a largo plazo” afirma Edgar Romeo. Siemens ha trabajado en estrecha colaboración con Cables RCT para desarrollar una solución personalizada que aborde los desafíos específicos que la empresa enfrenta en el día a día, como son una segmentación de la red industrial que garantice la seguridad del sistema, que haga posible el acceso a las máquinas desde el exterior de manera segura y que a su vez permita la conectividad necesaria para habilitar la digitalización de los procesos.

“Esto ha implicado, en algunos casos, que tuviéramos que trabajar directamente a pie de campo en la fábrica para entender mejor cómo se están utilizando las máquinas y cómo se puede mejorar para aumentar la eficiencia y la seguridad” recuerda Ángel Ventura. Siemens también ha ayudado a Cables RCT a desarrollar nuevas estrategias y procesos que permiten una mayor seguridad y fiabilidad, lo que contribuirá a la sostenibilidad y el éxito a largo plazo de la empresa. En resumen, la solución que Siemens ha suministrado a Cables RCT ha permitido principalmente mejorar el nivel de seguridad en la red industrial y mejorar la seguridad y la fiabilidad de los accesos remotos a las máquinas, todo ello basándose en una arquitectura de referencia estándar escalable que les permitirá seguir añadiendo máquinas a la infraestructura existente. Adicionalmente la solución ha mejorado el método de acceso a las máquinas del personal de mantenimiento interno, ha permitido un notable ahorro de costes en tiempo y desplazamientos de los proveedores de maquinaria y también ha permitido la digitalización de los procesos de la planta. ●



La garantía del éxito del proyecto: la excelente colaboración entre Cables RCT y sus socios Siemens y Araelec. “Durante el proceso de planificación y ejecución del proyecto, Siemens se ha convertido en un verdadero socio para nosotros” Edgar Romeo junto con Carlos Bazán y Angel Ventura.

Repensando el enfoque de la seguridad en la automatización

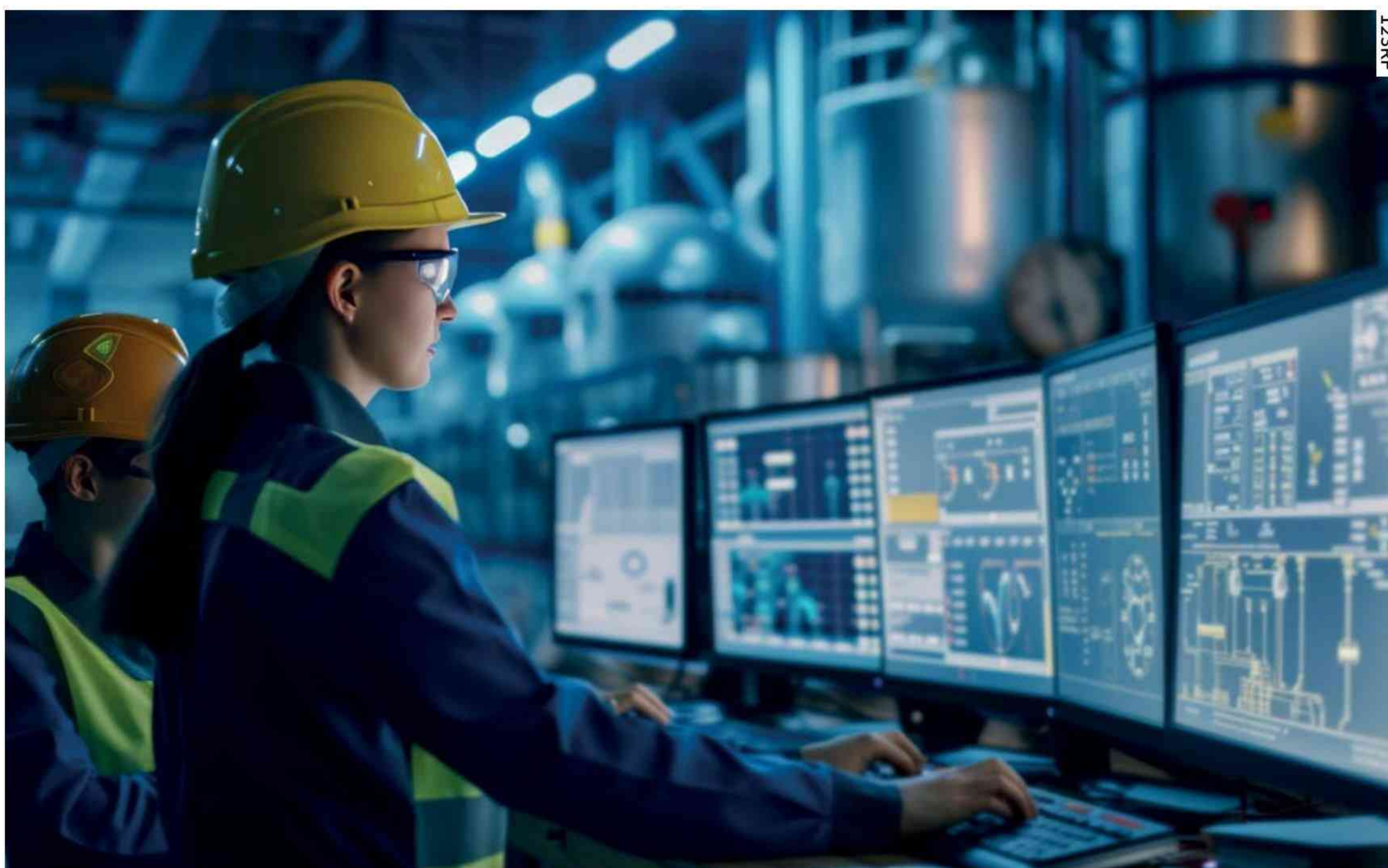
¿Y SI REDEFINIMOS LA TRIADA DE CIBERSEGURIDAD EN SISTEMAS OT?

En un mundo donde la interconexión de los sistemas de Tecnologías de la Operación (OT) es cada vez más evidente, es fundamental revisar y actualizar nuestros enfoques de ciberseguridad. Aunque la Triada C-I-A (Confidencialidad, Integridad y Disponibilidad) ha guiado históricamente nuestras estrategias, este artículo sugiere la adopción de un nuevo modelo: Información-Control-Configuración (I-C-S). Este marco no solo prioriza la disponibilidad, sino que también enfatiza la seguridad en la gestión de datos, la supervisión de procesos y la configuración de sistemas. Adoptar este enfoque integral es esencial para salvaguardar nuestras infraestructuras críticas en un panorama de amenazas en constante evolución.

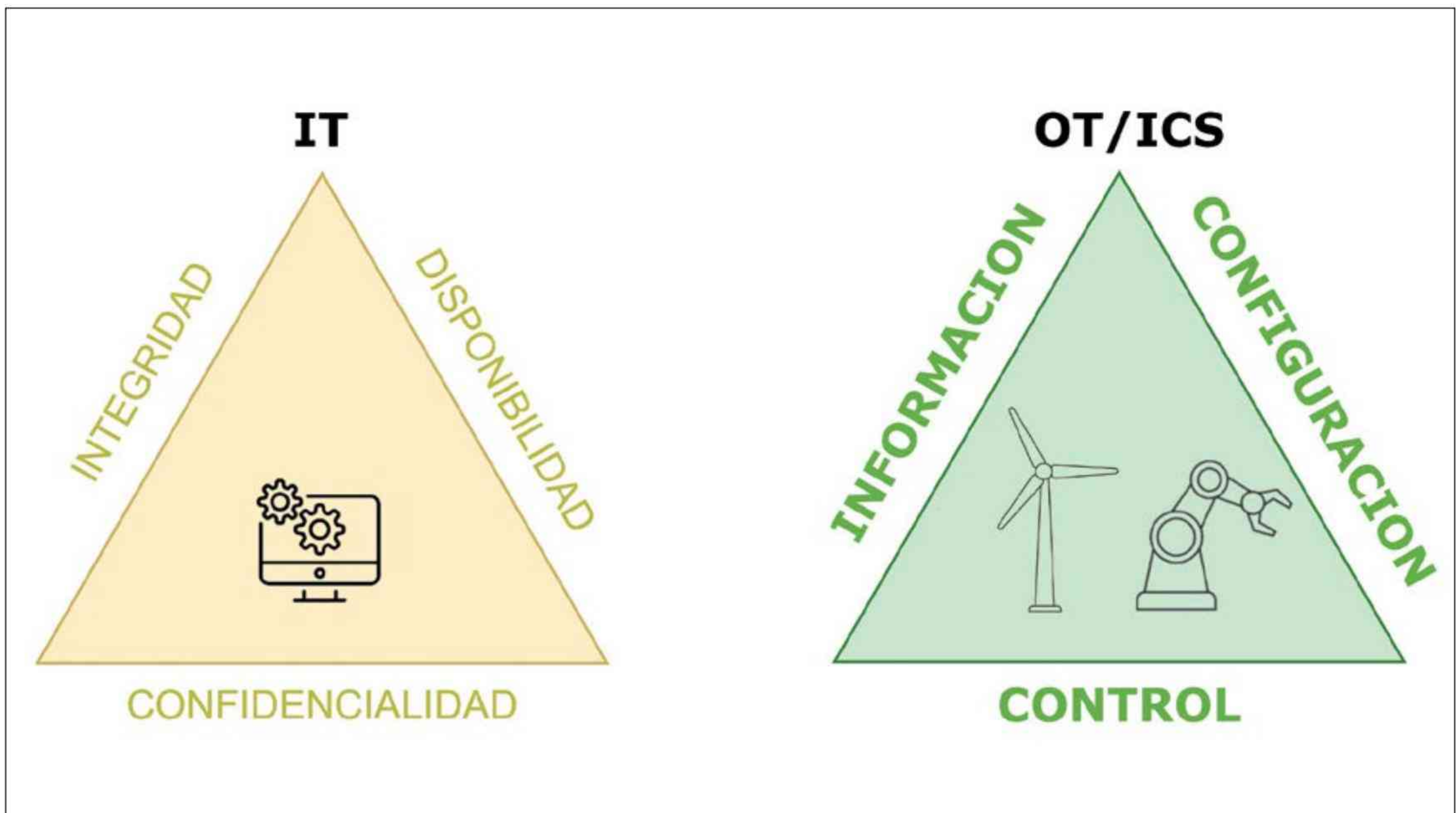
■ **Agustín Valencia**, OT/ICS/xIoT Cyber Security Business Development, Fortinet.

Manuel Ballesteros, Cyber Security OT Engineer, Siemens-Gamesa.

Miembros del Grupo de Trabajo de Ciberseguridad Industrial ISA – Spain Chapter. —✎



123RF



¿Redefinir la Triada de Ciberseguridad al hablar de OT?

Normalmente hablamos en ciberseguridad de la Triada C-I-A por sus palabras en inglés, *Confidentiality-Integrity-Availability* (Confidencialidad-Integridad-Disponibilidad). Y siempre se ha comentado como la principal diferencia entre OT (Tecnologías de la Operación) e IT (Tecnologías de la Información) es cómo la confidencialidad de la información prima en IT, mientras que en OT la disponibilidad del sistema suele ser primordial debido a la necesidad de mantener operaciones continuas. Esto es, en esencia, correcto, pero quizás tenemos que ir a otro nivel para que los parámetros sean más “accionables”, que haya una relación entre cómo se opera y programa un sistema de control y unos parámetros con los que compararlos. No olvidemos que la ciberseguridad en sistemas de automatización y control se ha vuelto crítica desde que somos conscientes de cuánto están interconectados estos sistemas pese a no haber sido diseñados originalmente con la seguridad en mente. Stuxnet. allá por 2010, el malware que paralizó el programa nuclear iraní modificando controladores y SCA-DA de Siemens, nos hizo ver que se requería prestar gran atención a las defensas de los activos.

Desde entonces, hemos vivido otros ataques que nos han ayudado a entender, tanto los vectores de entrada como los posibles impactos. Por ejemplo, ataques avanzados a sistemas de seguridad instrumentada (SIS) –que se pensaban invulnerables porque ya incorporaban muchas buenas prácticas en cuanto a control de configuración y validación de datos– hasta ataques, no exactamente contra sistemas OT, pero que paralizaron la operativa del mayor oleoducto del país. Además, desde el mundo de la automatización, siempre se ha tenido mucho más conocimiento del ámbito de programación y análisis de fallas desde dicho entorno, el que da la estación de ingeniería, que de su traslación al tráfico industrial, que analizan expertos de redes, pero no necesariamente con conocimientos de su implicación en estos sistemas. Por estas cosas, es bueno hacer una aproximación que permita un adecuado entendimiento entre las partes involucradas, tanto de cara al diseño, como a las protecciones de ciberseguridad como a la respuesta ante incidentes. Esta necesidad de un enfoque más integral se refleja en el modelo de *Información-Control-Configuración* y que bien podría ser *I-C-S* por las siglas en inglés, *Information-Control-Set Up*.

¿Por qué es importante esta diferenciación?

En la actualidad, muchas empresas están acometiendo proyectos de segmentación de redes OT, junto con controlar el inventario de dispositivos. El problema es acometerlo de manera efectiva y de ahí este artículo. En muchos casos la segmentación no va más allá de qué puede hablar con qué; sin embargo, sin ir a nivel de protocolo industrial, un fallo de configuración en una modificación de la red, o accesos remotos desde equipos comprometidos, pueden sobrepasar estas defensas. El siguiente paso es restringir las comunicaciones a los protocolos autorizados. Aunque hay diversidad de protocolos industriales, quizás podríamos identificar algunos que son los que mayoritariamente se encuentran en las industrias e IoT: Profinet & Profibus, OPC, Modbus y MQTT. Aun así, cada vez hay más artículos que referencian cómo están evolucionando ataques y pruebas de concepto a partir de abusar del protocolo industrial. No olvidemos que Stuxnet ya lo hacía y fue capaz de cambiar los *setpoints* de velocidad de centrifugadoras para que trabajaran en frecuencia crítica, que modificó la lógica de las válvulas de venteo

para que no abrieran en las descargas y las líneas quedaran obstruidas y también modificó láminas de SCADA para que los operadores no pudieran observar la velocidad real de las centrifugadoras atacadas ni ver si estas habían disparado.

¿Cuál es el problema?

Que dejando la comunicación del protocolo para solamente tomar datos, alguien podría parar el sistema o cambiar la configuración del mismo. Por eso, es crucial no solo segmentar las redes y controlar el acceso, sino también implementar controles estrictos sobre qué protocolos pueden ser utilizados y bajo qué condiciones, asegurando que cada comunicación sea legítima y segura.

● **Información:** Se refiere a la recopilación de datos de los sistemas para monitoreo, análisis y optimización, crucial en la Industria 4.0. Y así hacer casos de uso tan variados como optimizar la producción, mantenimiento preventivo, hasta gemelos digitales que permitan evaluar el funcionamiento dinámico del sistema en distintos escenarios. En muchos casos se utiliza un *gateway* que convierte el protocolo industrial en el utilizado para subir a un repositorio de datos, mayoritariamente MQTT.

Es fundamental garantizar que la información recopilada sea precisa y esté protegida contra alteraciones.

● **Control:** Todas las acciones que hace un operador de planta para gestionar los sistemas de control. Parar o arrancar equipos, abrir o cerrar válvulas o interruptores, o cambiar la consigna de funcionamiento de un sistema automático (velocidad de la línea, caudal, nivel de calderines, pH del producto, etc). La seguridad aquí se centra en asegurar que solo los operadores autorizados puedan realizar estas acciones y que las comunicaciones no sean interceptadas o manipuladas.

● **Configuración (set-up en Inglés):** Todas las gestiones que hace el personal de ingeniería o mantenimiento. Desde crear lazos de control, modificar límites de protección de funcionamiento o cargar programas completos implicando todo lo anterior. Las consecuencias en estos casos pueden ser catastróficas, tanto para la instalación como para la calidad del producto resultante, como causar daños físicos o financieros significativos. En el primer grupo podríamos hablar de modificar límites de temperatura o presión a las que funcionan calderas o columnas de destilación, límites de velocidad que afectarían a turbinas -térmicas o eólicas- pero también parámetros eléctricos con los que atacar el sistema de transporte o distribución eléctrica.

En el segundo grupo hablaríamos de sectores como el agua, farmacéutico o alimentario, donde las alteraciones implicarían la insalubridad de los productos y si, estos ataques se podrían realizar tanto contra los equipos que producen las mezclas como con los equipos que protegen de los valores no pasan de los límites de seguridad. Desde el concepto de seguridad de red, esta diferenciación se encuentra en la denominada “Capa 7” o “Capa de aplicación” (según el modelo estándar de capas de comunicación de OSI -*Open Systems Interconnection*-, no confundir con los niveles de la pirámide de automatización -ISA95 o modelo de Purdue-). Para la triada propuesta de Información-Control-Configuración, evaluamos el estándar de comunicación industrial PROFINET. Recordemos que facilita la integración de dispositivos de campo como sensores y actuadores con sistemas de control, permitiendo un intercambio rápido y confiable de datos. Admite comunicaciones cíclicas y acíclicas, proporcionando flexibilidad para el control en tiempo real y la transferencia de datos diagnósticos, utilizando la capa 7 para aplicaciones y la capa 5 para la gestión de sesiones de datos.

Podríamos evaluar la defensa de nuestros activos con la siguiente tabla:

Function type			Function name	Function code	Comment	
Data Access	Bit access	Physical Discrete Inputs	Read Discrete Inputs	2		
		Internal Bits or Physical Coils	Read Coils	1		
			Write Single Coil	5		
			Write Multiple Coils	15		
	16-bit access	Physical Input Registers	Read Input Registers	4		
		Internal Registers or Physical Output Registers	Read Multiple Holding Registers	3		
			Write Single Holding Register	6		
			Write Multiple Holding Registers	16		
			Read/Write Multiple Registers	23		
			Mask Write Register	22		
			Read FIFO Queue	24		
			File Record Access	Read File Record	20	
				Write File Record	21	

Información

Control

Configuración

Información

Control

Configuración

Triada	Descripción	Ejemplo en PROFINET	Consideraciones de Seguridad
Información	Recopilación y transmisión de datos operativos para monitoreo y análisis.	Lectura de datos (registros alarmas/status data) de sensores y actuadores a través del nombre único que lo identifica. Transmisión de información de estado del sistema a sistemas SCADA.	Asegurar la integridad de los datos para evitar manipulaciones. Implementar autenticación para acceso a datos.
Control	Ejecución de comandos operativos que afectan directamente los procesos de producción.	Envío de comandos para iniciar/parar motores. Ajuste de parámetros operativos, como velocidad o temperatura.	Limitar el acceso a operadores autorizados. Implementar controles de acceso y auditoría/logs de comandos enviados.
Configuración	Ajuste de parámetros del sistema y actualización de <i>software/firmware</i> para la operación adecuada.	Configuración de dispositivos PROFINET - IO-Controllers, IO-Devices o IO-Supervisors para tareas de producción. Topología de red. Tiempo real o IRT. Actualización de <i>firmware</i> de controladores.	Proteger el acceso a las configuraciones críticas. Utilizar autenticación multifactor y cifrado para cambios de configuración.

¿Hacia dónde debemos dirigirnos?

Debemos avanzar a hacer un control granular sobre los protocolos industriales y determinar qué usuarios tienen permiso para cada grado de privilegio.

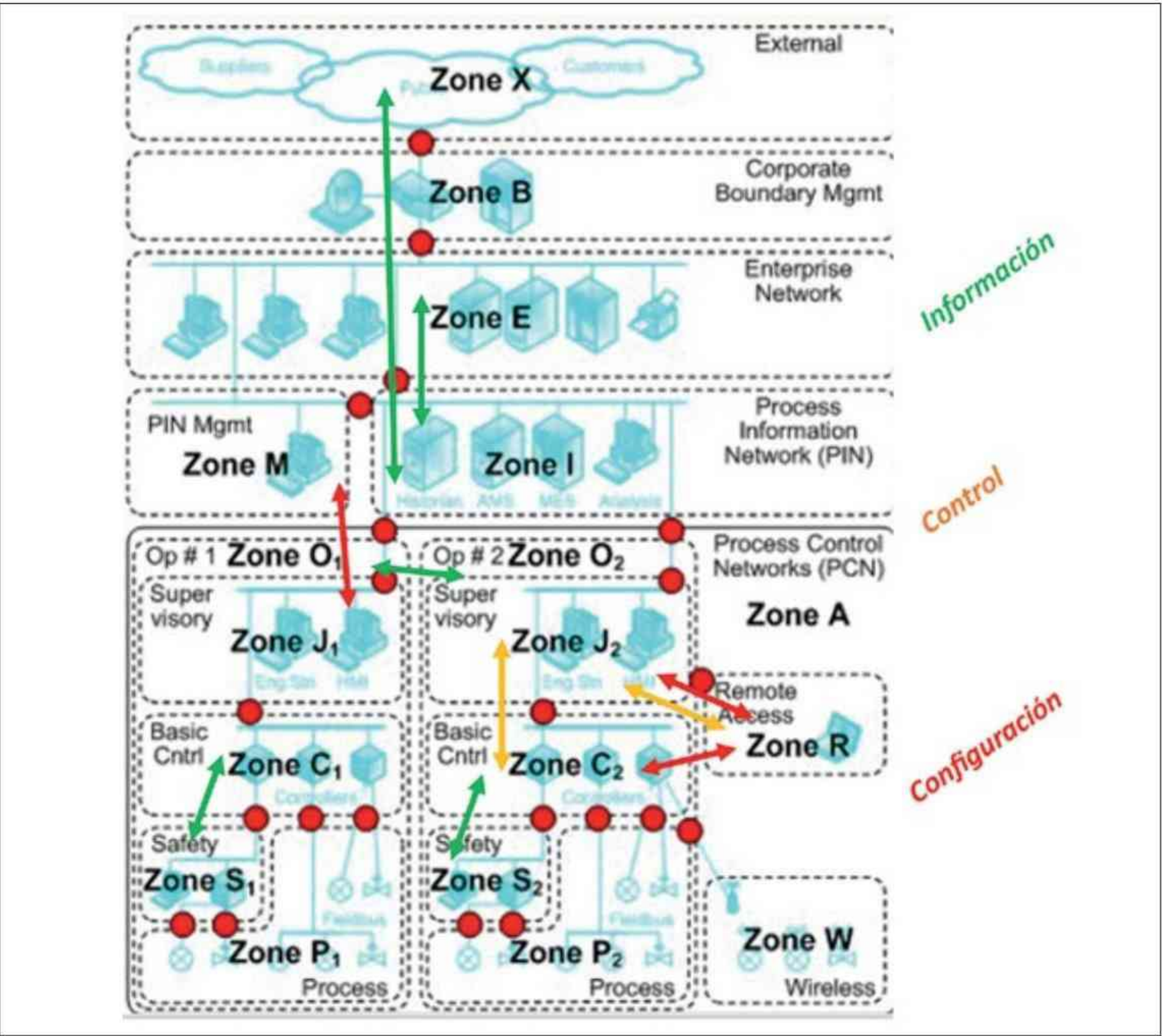
Esta práctica está asentada en los principales fabricantes de control distribuido (DCS), sistemas instrumentados de seguridad (SIS) y sistemas SCADA, sin embargo, daba lugar a la falsa creencia de que hacer cambios en los controladores no era posible sin pasar por dichos sistemas.

No olvidemos que un controlador normal tradicionalmente responde a todas las peticiones de quienes llegan hasta ellos, y es por eso que se ha de poner un nivel adicional a nivel de control de red.

Algunos *firewalls* de nueva generación permiten esta granularidad en el control de los distintos comandos dentro del protocolo industrial. Por ejemplo, las operaciones de “lectura” de archivos de configuración deben estar estrictamente limitadas a aquellos usuarios que tengan autorización explícita para realizar

cambios de configuración. Aunque conceder permisos de “solo lectura” puede parecer una buena práctica de seguridad, sin un control granular adecuado, estos permisos pueden

convertirse en un vector de ataque, permitiendo a actores malintencionados acceder a información sensible y potencialmente comprometer la seguridad del sistema.



Por último

Esta propuesta no es normalmente comentada pero tampoco puede considerarse disruptiva. Se trata de destacar y dar más importancia a conceptos comunes dentro del mundo de la

automatización y de la ciberseguridad en entornos OT desde el punto de vista de los conceptos que manejan los equipos de automatización y control. Además, para demostrar el valor añadido de esta propuesta y ayudar

al lector, cabe destacar que está claramente alineada con las familias de controles definidos en la norma ISA/IEC 62443-3-3. Algunos de los controles relevantes se incluyen en la siguiente tabla:

Foundational Requirement	Security Requirement	Triada Relacionada	Descripción
FR1: Identification & Authentication	SR 1.1: Identification and Authentication Control	Información, Configuración	Asegura que solo usuarios y dispositivos autorizados puedan acceder a datos críticos y modificar configuraciones del sistema
	SR 1.3: Authentication of Software and Information	Información,	Verifica la autenticidad de software y datos para evitar manipulaciones
FR2: Use Control	SR 2.1: Authorization Enforcement	Control, Configuración	Garantiza que solo los usuarios autorizados puedan ejecutar comandos.
	RE 2: Permission Mapping to Roles	Control, Configuración	Define claramente qué acciones pueden realizar distintos roles dentro del sistema.
	SR 2.12: Non-Repudiation	Control, Configuración	Asegura que todas las acciones realizadas en el sistema sean trazables y verificables.
FR3: System Integrity	SR 3.1: Communication Integrity	Información, Control	Protege la integridad de las comunicaciones para evitar que los datos y comandos sean interceptados o alterados
	SR 3.2: Malicious Code Protection	Información, Control, Configuración	Previene la introducción de software malicioso y comprometer la integridad del sistema.
	SR 3.5: Input Validation	Control, Configuración	Asegura que todas las entradas en el sistema sean válidas y no dañinas.
FR5: Restricted Data Flow	SR 5.1: Network Segmentation	Información, Control, Configuración	Limita el flujo de datos entre las zonas autorizadas a comunicar, y con los perfiles autorizados
	RE 2: Independence from Non-Control System Networks	Información, Control, Configuración	Asegura que los ICS estén aislados de redes externas no seguras pero cobra más sentido con la diferenciación que proponemos.
	SR 5.2: Zone Boundary Protection	Información, Control, Configuración	Define y protege los límites entre diferentes zonas de la red para evitar movimientos laterales de posibles atacantes.



EDICIONES TÉCNICAS



Motor de Ventas Ediserv

Primer Grupo de Prensa Profesional Especializado

NUESTROS CANALES DE DIFUSIÓN:

- ✓ Revista en Papel
- ✓ Revista Digital
- ✓ Web
- ✓ Newsletters
- ✓ Redes Sociales

**PUBLICACIONES MULTIPLATAFORMA
CON CINCO PILARES QUE GARANTIZAN
UNA VISIBILIDAD DEL 100%**

NUESTRAS PUBLICACIONES:

AUTOMATIZACIÓN Y TECNOLOGÍA

Automática e Instrumentación

www.automaticaeinstrumentacion.com

CONSTRUCCIÓN

CIC Arquitectura y Sostenibilidad - www.cicconstruccion.com

ClimaNoticias - www.climanoticias.com

ElectroNoticias - www.electronoticias.com

POSVENTA DE AUTOMOCIÓN

Talleres en Comunicación - www.posventa.info

Posventa de Automoción.com - Chapa y Pintura, Neumáticos y Mecánica Rápida, Nuestros Talleres, Recambios y Accesorios

www.posventa.com

HOSTELERÍA Y RESTAURACIÓN

Hostelería, Diseño, Equipamiento, Food Service & Beverage

www.revistahosteleria.com

DISTRIBUCIÓN

Aral - www.revistaaral.com

BeautyProf - www.revistabeautyprof.com

Nueva Ferretería - www.nuevaferreteria.com

INDUSTRIA

AutoRevista - www.auto-revista.com

Metales & Metalurgia-Máquinas - www.metalesymaquinas.com

Óleo - www.oleorevista.com

Revista PQ - www.revistapq.com

LOGÍSTICA Y TRANSPORTE

Autobuses & Autocares - www.autobusesyautocares.com

Logística Profesional - www.logisticaprofesional.com

Todotransporte - www.todotransporte.com

SANITARIO

DM Dentista Moderno - www.eldentistamoderno.com

☎ 91 297 20 00

Oriental Motor apuesta por nuevas estrategias para simplificar la programación y mejorar la eficiencia en robótica

CONSEJOS EN EL DESARROLLO DE ROBOTS EN LA AUTOMATIZACIÓN Y OPTIMIZACIÓN DE PROCESOS

El desarrollo de robots para la automatización está en auge, impulsado por la necesidad de optimizar procesos y reducir costos. Sin embargo, integrar estas tecnologías en líneas de producción existentes presenta desafíos. Soluciones innovadoras buscan simplificar la programación y el control de robots, permitiendo a las empresas diseñar, implementar y mantener sus propios sistemas. Estas herramientas mejoran la eficiencia operativa y reducen los tiempos de inactividad, adaptándose a diversas configuraciones robóticas y aumentando el rendimiento en sectores industriales clave.

■ Oriental Motor

Contra la creciente demanda de robots, muchas empresas buscan instalar robots sobre líneas de producción ya existentes, lo cual es difícil de cubrir a través de las soluciones en el mercado actuales. En estos casos la solución pasa por soluciones de fabricación propia. A la hora de automatizar nuevos procesos y para resolver esta demanda, Oriental Motor recomienda el desarrollo de procesos de producción centrados en la reducción de costes, el ahorro de espacio y, especialmente, la reducción de la carga de programación.

Con el objetivo de facilitar el diseño, las pruebas y la implementación de robots de desarrollo propio, Oriental Motor ha desarrollado el controlador de robot MRC01 y el software de programación MRC Studio para accionamientos de la familia AZ Alpha Step, eliminando barreras incluso para aquellos diseñadores de equipos que realizan este tipo de proyectos por primera vez.

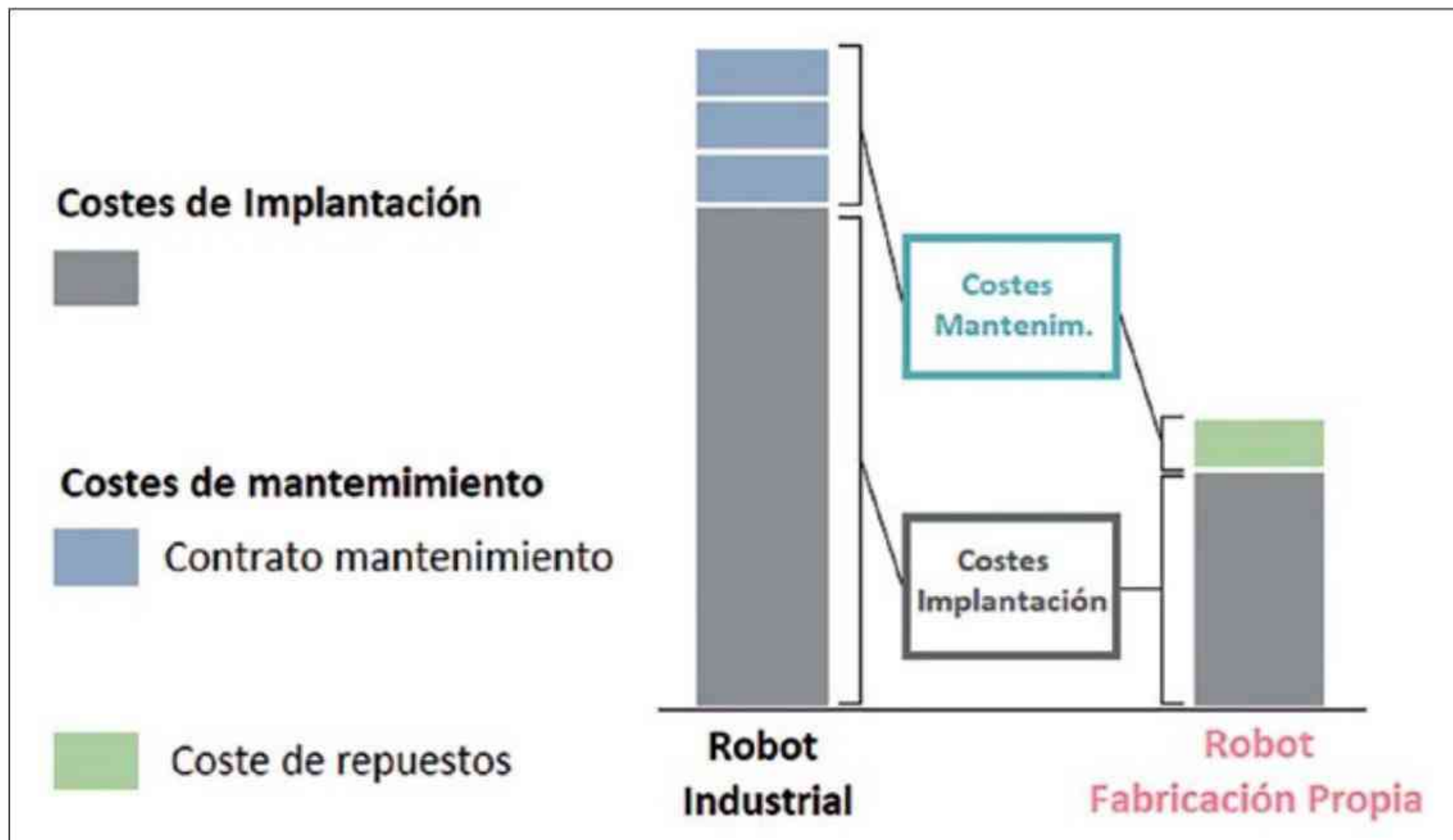


MRC01 and MRC Studio.

Ahorro en mantenimiento y propiedad

El coste inicial no solo conlleva el coste de implantación del robot. En caso de malfuncionamiento es bastante habitual recurrir al fabricante o a una compañía externa para realizar tareas de mantenimiento, lo que se traduce en tiempo y dinero. La fabricación propia de estos

robots reduce los costes de mantenimiento después de la implantación y por lo tanto el coste total de propiedad. Cuando el desarrollo es propio, son los empleados los que pueden identificar las causas de fallo y proceder al remplazo de componentes, reduciendo el tiempo de parada en caso de fallo del robot hasta la nueva puesta en marcha.



Comparativa de costes entre un robot industrial y un robot de fabricación propia.

Programación simplificada

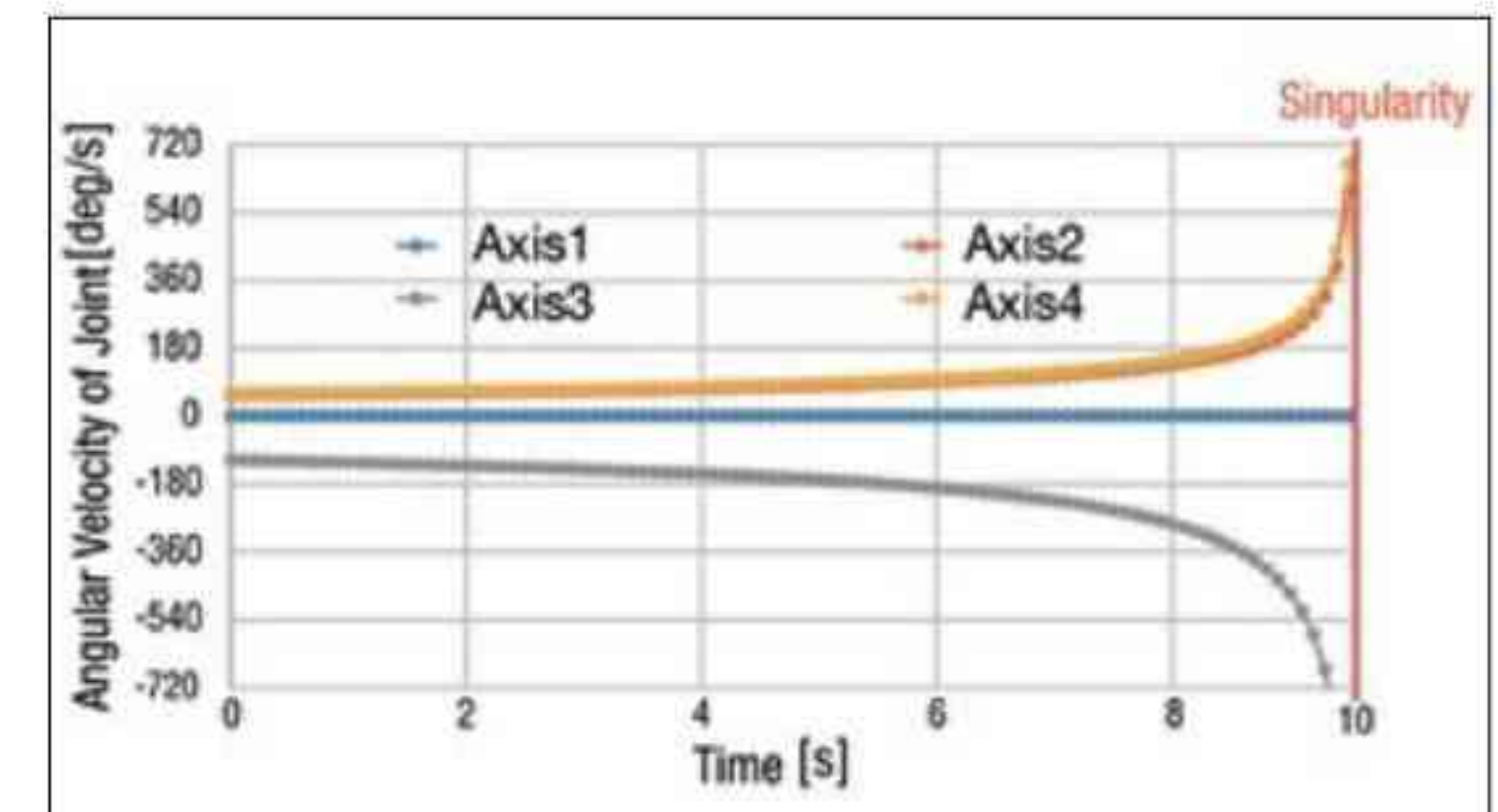
La dificultad de programación y control de ejes múltiples interrelacionados son un impedimento en la construcción de robots. La función del controlador del robot es desarrollar la posición, velocidad y trayectoria del 'punto central de la herramienta' o TCP (tool central point) según se desee, olvidándonos del control individual de cada motor que acciona cada articulación del robot. Esto conlleva cálculos cinemáticos que no son sencillos y que dependen de la estructura (número de ejes, dimensiones de brazos) y tipo de robot (SCARA, articulado vertical, cartesiano), de modo que cuanto más complejo sea, más complicados son estos cálculos. Debe ocuparse, además, de la selección del sistema de coordenadas adecuado según el tipo de robot y operación a la hora de

enseñar las posiciones y movimientos que debe realizar la mano y el efector final. El controlador MRC01 permite la elección de estos sistemas y la definición y dimensiones de elementos en las operaciones de enseñanza del robot.

Los perfiles de velocidad y ángulo de cada articulación constituyen básicamente un cálculo complejo que cambia en el tiempo. De modo que en el control del robot es esencial un avanzado control de movimiento para poder operar los motores sincronizadamente en cada sección de acuerdo con el perfil de posicionamiento.

Por otra parte, cuando todos los elementos se controlan mediante PLC, es necesario desarrollar simultáneamente la cinemática y creación de programas del robot y equipos periféricos, incrementando la carga de

trabajo del programador del PLC. La utilización del controlador MRC01 junto con el software MRC Studio permite crear programas de movimiento del robot y testarlos independientemente del controlador principal. Esto permite mejorar la eficiencia en la puesta en marcha del equipo, dado que se pueden repartir las tareas del robot y PLC entre diferentes personas.

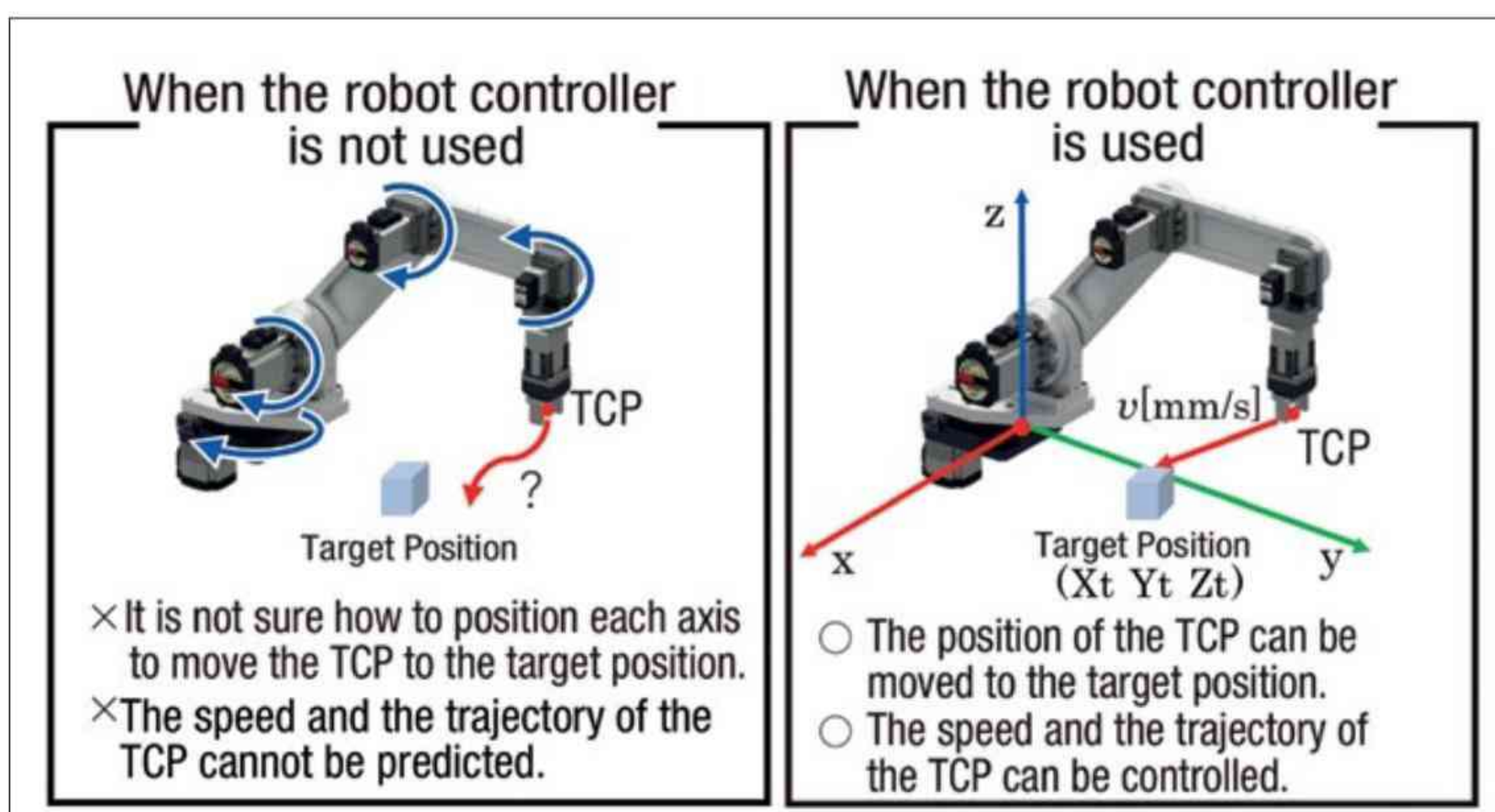


Cambios en la velocidad de las articulaciones cerca de la singularidad de un robot articulado vertical de 4 ejes.

Protección ante singularidades

Otra de las dificultades en el desarrollo del robot que debe tenerse en cuenta es el estudio de aquellas posiciones no controlables de la estructura del propio robot, denominadas singularidades, que hacen que la velocidad se incremente al acercarse a estos puntos haciendo el movimiento incontrolable. El controlador MRC01 dispone de la función 'Singularity protective function' que para la operación y notifica mediante una alarma antes de que el robot se aproxime a la singularidad, además de otras funciones de seguridad como el 'Slip Mode', que tienen en cuenta la desviación de posición, en caso de contacto con otros equipos y personas, así como límites de posición y velocidad.

Oriental Motor ofrece un controlador de robot con un software de programación fácil de manejar para desarrolladores sin experiencia previa en el control de robots. Reduciendo la curva de aprendizaje ya que independientemente del diferente tipo de robot, sea cartesiano, SCARA o de articulación vertical, el modo de operación del software MRC Studio así como la conexión y modos de comunicación entre el PLC y el controlador MRC01 son los mismos. ●

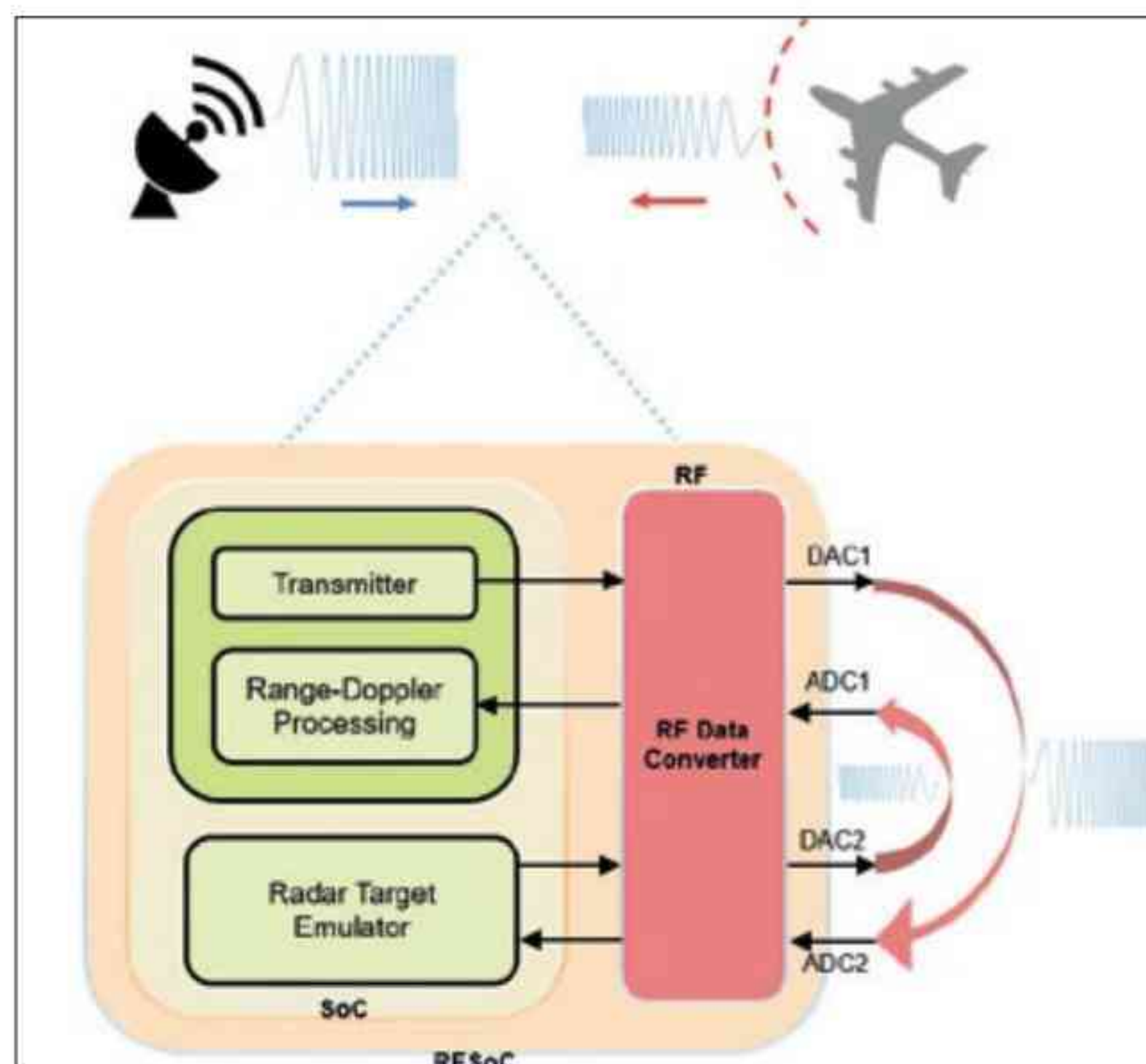


Funcionamiento del robot.



Versión R2024b de MATLAB y Simulink

MathWorks presenta el lanzamiento de la versión R2024b de las líneas de productos de MATLAB y Simulink que incorpora varias actualizaciones principales que agilizan los flujos de trabajo de equipos de ingeniería e investigación que trabajan en sistemas de telecomunicaciones, sistemas de control y aplicaciones de procesamiento digital de señales. Además de mejoras en productos de la plataforma de la compañía, esta nueva versión incluye actualizaciones principales de herramientas de MATLAB y Simulink populares, como las siguientes: 5G Toolbox, DSP HDL Toolbox, Simulink



Control Design, System Composer y un nuevo paquete de soporte de hardware.

“La capacidad de una organización de ofrecer productos de alta calidad, fiables y seguros subraya el papel crítico de la simulación y el diseño basado en modelos”, afirma Andy Grace, vicepresidente de automatización de diseño de MathWorks. “Las mejoras de la versión R2024b están diseñadas para escalar, automatizar y agilizar aspectos clave del flujo de trabajo, y ayudar a equipos de ingeniería a optimizar el rendimiento y fiabilidad de los sistemas”.

www.mathworks.com

Switches DGS-1250 con cuatro puertos SFP+ a 10 Gigabit



D-Link lanza su gama de Switches Smart Managed DGS-1250, que destaca por disponer de cuatro puertos SFP+ a 10 Gigabit, de forma que los enlaces ascendentes hacia los switches de agregación/distribución o bien al núcleo de red, acceso a Internet o servidores, se realiza con un ancho de banda de 10 Gigabit, permitiendo así el máximo rendimiento en los accesos a la red e Internet en los dispositivos conectados a estos switches (ordenadores, puntos de acceso WiFi para la red inalámbrica, etc). La familia de conmutadores DGS-1250 es adecuada para las redes informáticas empresariales que necesiten enlaces ascendentes a 10 Gigabit, bien por cobre o por fibra óptica para cubrir largas distancias, a costes muy asequibles y con densidades de 24 o 48 puertos Gigabit, así como múltiples opciones PoE (con hasta 370W de PoE Budget) para simplificar las instalaciones al unificar datos y alimentación por el mismo cable de red cuando se conectan dispositivos compatibles Power Over Ethernet como puntos de acceso Wi-Fi, cámaras o teléfonos IP, etc. Otro aspecto de los DGS-1250 es su gestión de red con funcionalidades como Multiple Spanning Tree, Link Aggregation Protocol y Routing Estático en capa 3 para aumentar el rendimiento, seguridad y redundancia de la red.

www.dlink.com

Nuevo motor eléctrico W23 Sync+



WEG ha lanzado su serie de motores W23 Sync+ que destaca por integrar imanes permanentes (PM) –con imanes de ferrita o de neodimio–, y la reluctancia sincrónica, también llamada magnética, (SynRM), proporcionando un mayor rendimiento en toda la gama de velocidades respecto a los motores de inducción convencionales. Javier de la Morena, responsable de grandes cuentas y marketing de WEG Iberia, explica las ventajas de la tecnología del motor síncrono de reluctancia magnética (PMSynRM): “WEG se anticipa habitualmente a los nuevos reglamentos y normas internacionales, y su nueva serie de motores W23 Sync+ es un ejemplo más de ello. La búsqueda de eficiencias muy elevadas, actualmente hasta la clase IE6, les impulsó a esta innovación. Es por ello que los motores W23 Sync+ cumplen o exceden los requisitos mínimos actuales del reglamento europeo relativo al diseño ecológico, el cual estipula que los nuevos motores eléctricos deben cumplir, al menos, unas eficiencias IE3 o IE4 dependiendo de las potencias. Actualmente, el motor IE6 de WEG es el W23 Sync+ ULTRA, mientras que los motores de clases IE3 a IE5 se encuadran en la serie general W23 Sync+”.

www.weg.net

Sensores adaptados para centros de microfulfillment

■ Leuze ofrece soluciones a medida para los centros de microfulfillment (MFC) con los que los comercios minoristas de alimentación responden a los cambios que experimenta la logística de distribución debido al aumento del comercio online, que exige gestionar los pedidos cerca del cliente.

Para el funcionamiento eficiente y automatizado de una MFC se requieren sensores especializados. Las principales tareas desarrolladas en un centro logístico de este tipo son la identificación, detección y protección. Los sensores utilizados deben ser muy pequeños porque en los MFC el espacio se aprovecha de manera extremadamente eficiente.

De esta manera, para las áreas de productos frescos y congelados, la Leuze ofrece sus sensores ópticos de las

series 3C y 25C, que funcionan de forma fiable incluso en el área de congelación y con movimientos rápidos. En el área estándar, ha desarrollado la conectividad integrada (Integrated Connectivity) para la serie BCL 300i. Esta función permite que el lector de código de barras fijo comunique directamente con el control sin necesidad de una interfaz externa. Finalmente, para la gestión de pedidos, aporta sus cortinas ópticas de seguridad ELC 100 de Leuze.



www.leuze.com

Módulo lineal de correa dentada drylin ZLX

■ El nuevo módulo lineal drylin ZLX de igus se caracteriza por ofrecer un funcionamiento silencioso, robusto y, como todos los módulos de la compañía, sin necesidad de lubricación. Su diseño se basa en el principio de deslizar en lugar de rodar. El sistema trabaja sobre una amplia superficie de contacto que, junto con una menor presión superficial, permite el uso de componentes de plástico y materiales más blandos (como el aluminio), lo que no sólo hace que el diseño sea más ligero, sino que también permite que funcione silenciosamente. El carro se desplaza sobre elementos deslizantes fabricados con el plástico iglidur J200, que ofrece una larga vida útil con ajustes tanto rápidos como lentos.



El material también dispone de lubricantes sólidos integrados que se liberan mientras el módulo está en funcionamiento, y permiten prescindir de la lubricación y las tareas de mantenimiento. Para mejorar el rendimiento, los diseñadores de producto han optimizado la relación entre las dimensiones del sistema de guiado y la desviación, mejorando la resistencia al desgaste de la correa dentada mediante radios de desviación mayores, ya que se somete a menos flexión y, por consiguiente, a menos tensión. Al mismo tiempo, el nuevo tamaño 16 de la guía lineal drylin W garantiza una mayor vida útil.

www.igus.es

Novedades en sistemas de sujeción de cables

■ norelem cuenta con cuatro nuevas familias de productos de sistemas de sujeción de cables con tecnología de cinta de fijación que ofrece soluciones rápidas y flexibles de agrupamiento y fijación. De esta manera, la compañía res-



ponde a la necesidad de una gestión eficaz del cableado para mantener un entorno operativo fluido y seguro, ya que unos cables bien organizados evitan riesgos, prolongan la vida útil de los equipos y minimizan el desorden. La base de fijación y el sistema de cinta están diseñados para atornillar hilos, cables o mangueras, lo que permite extraerlos e introducirlos sin necesidad de herramientas. La cinta se puede abrir y cerrar en numerosas ocasiones, además de ser apta para montaje directo con tornillos avellanados. Disponible en anchuras de 7,5, 10, 20 y 30 mm, con longitudes que admiten rangos de sujeción de 4 a 100 mm, esta solución adaptable para la gestión de cables permite realizar ajustes y reposicionamientos sin herramientas adicionales, garantizando la rentabilidad y la conciencia medioambiental.

La compañía también ofrece una base con cinta de fijación diseñada para el montaje en perfiles de aluminio de tipo I y tipo B. Esta versión puede fijarse transversal o paralelamente a la ranura del perfil con un giro a la derecha de 45°. Disponible en anchuras de 10 y 20 mm y tres longitudes, esta base admite rangos de sujeción de 4 a 60 mm.

www.norelem.es

Nueva solución de refrigeración de megavatios para la IA

■ Rittal ha presentado su nueva solución de refrigeración que ofrece más de un megavatio de potencia de refrigeración para allanar el camino para la IA. La necesidad de potencia de procesamiento está creciendo tanto que se requiere un nivel completamente nuevo de escalabilidad, refrigeración, distribución de corriente y eficiencia energética. El proveedor se adentra en el nuevo campo en auge de la refrigeración de la TI, en lo que respecta a la clase de potencia y la tecnología.

La densidad de potencia para las aplicaciones de IA, como el entrenamiento y la operación de grandes modelos lingüísticos (LLM) en los centros de datos del futuro o la ya extendida computación de alto rendimiento, están haciendo que la refrigeración por ai-



re habitual llegue rápidamente a sus límites físicos y económicos. Los nuevos procesadores gráficos (GPU) ultrarrápidos producen tanto calor que los fabricantes los están diseñando para una potente refrigeración por líquido directa.

En consecuencia, la compañía ha desarrollado una solución de refrigeración modular a través de una estrecha colaboración con varios hiperescaladores que, mediante una refrigeración por agua directa, ofrece una potencia

de refrigeración de más de 1 MW y con ello permite alcanzar las densidades de potencia necesarias.

www.rittal.com

Nuevo elemento de mando PIT oe ETH

■ Pilz presenta su nuevo elemento de mando PIT oe ETH equipado con un puerto Ethernet activable que protege contra el acceso no autorizado a interfaces Ethernet libremente accesibles en entornos industriales. La compañía aumenta así su gama de dispositivos de mando y diagnóstico.



Este componente protege la red, el know-how, los datos y la inversión de máquinas e instalaciones. El nuevo interfaz Ethernet funciona como cortafuegos y protege contra el acceso no autorizado desde el exterior a las conexiones de red y contra el acceso directo interno a Human Machine Interfaces y datos de control. De este modo, permite determinar de manera clara y segura quién, cuándo y cómo puede acceder a datos sensibles de una máquina, con el fin de aumentar la seguridad de la producción.

En combinación con la unidad de lectura PITreader de Pilz, la interfaz Ethernet solo se puede activar si se dispone de la correspondiente autorización. Es decir, solo las personas autorizadas pueden utilizar temporalmente estas interfaces para crear nuevas configuraciones, programas o copias de seguridad, por ejemplo. Al disponer de entradas estándar de 24 o 5 voltios, es posible activarlas de forma flexible a través de cualquier salida de control, proporcionando a los usuarios un control completo del flujo de datos en sus redes.

www.pilz.com

Sistema de conexión enchufable RST



■ Wieland Electric ha dado a conocer su nuevo catálogo 'Safe and Sure' en el que especifica todas las funcionalidades y aplicaciones de su sistema de conexión enchufable RST con el que ofrece soluciones efectivas en entornos críticos y exigentes.

Este sistema está diseñado para instalaciones que requieren un alto grado de protección y durabilidad en condiciones adversas. Ya sea en naves industriales, carreteras, aparcamientos, invernaderos o zonas al aire libre, garantiza un rendimiento óptimo.

Con el más alto grado de protección IP, el sistema es resistente a constantes cambios de temperatura, alta radiación UV y desgaste mecánico.

Entre la variedad de aplicaciones se encuentran: horticultura, fabricación de maquinaria, plantas industriales, edificación, sistemas fotovoltaicos, aerogeneración, iluminación para eventos, construcción naval, infraestructuras, iluminación exterior o entornos ATEX.

www.wieland-electric.es

Medidor ultrasónico para caudales de bajo volumen en redes de alta presión

■ SICK ha presentado en el mercado su nuevo medidor ultrasónico FLOWSIC550, con el que amplía la gama de medidores ultrasónicos y ha sido especialmente diseñado para aplicaciones de alta presión en la distribución de gas natural con diámetros nominales pequeños. Este medidor cumple con los requisitos de precisión de la norma OIML R 137 1&2 y el informe AGA 9 de 2022, lo que permite una facturación precisa incluso de los caudales de bajo volumen, especialmente en aplicaciones de distribución y transporte de gas natural. En las estaciones de transferencia y medición, este dispositivo, prácticamente libre de



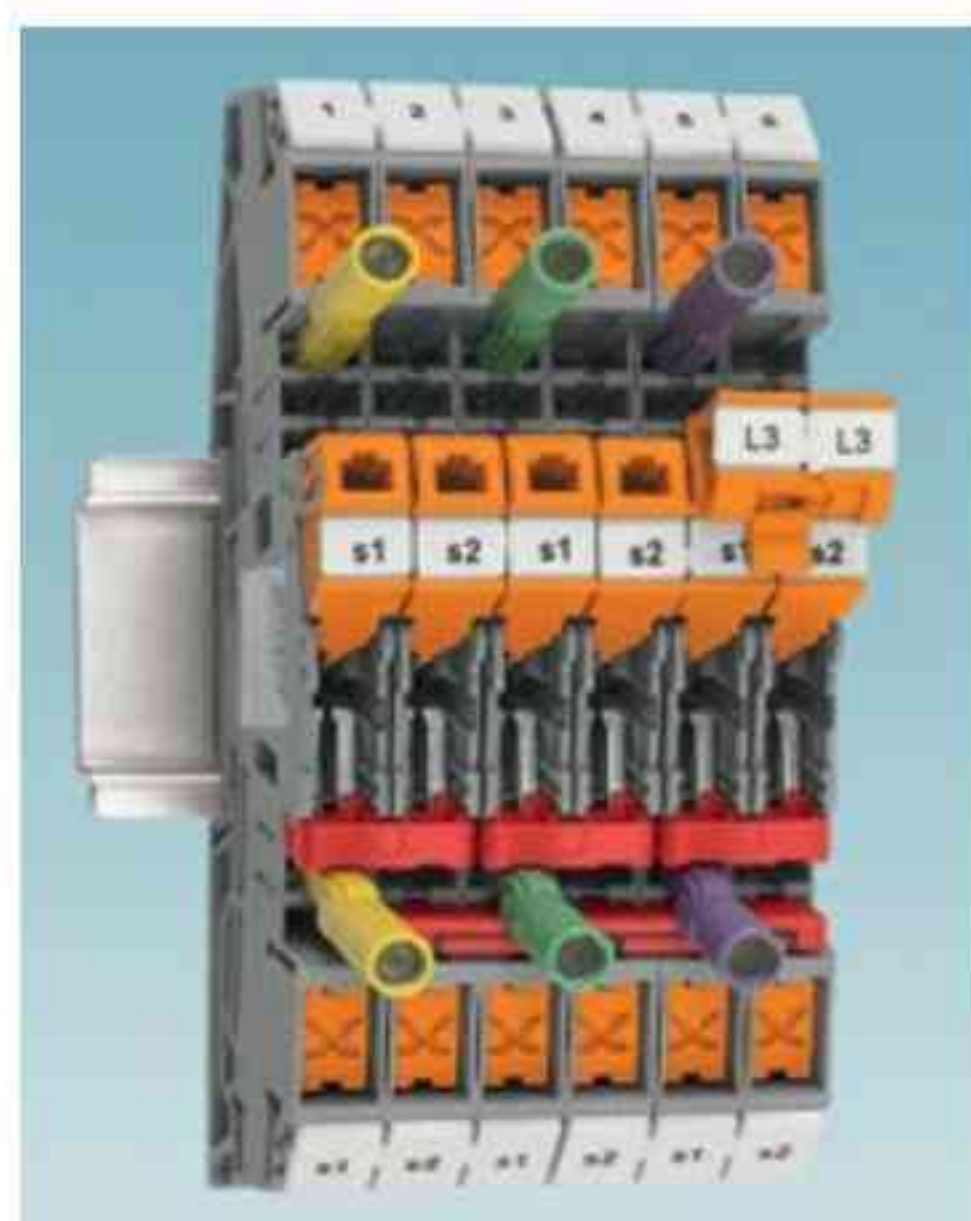
mantenimiento gracias a su tecnología de medición sin contacto, reduce los costes operativos en el punto de medición y asegura un suministro de gas continuo y sin problemas.

Además de medir caudales de bajo volumen en redes de alta presión, es adecuado para numerosas otras aplicaciones: mediciones en redes de distribución y transporte de gas natural, almacenamiento de gas natural, estaciones de transferencia, mediciones en consumidores industriales de gas a alta presión y, en general, donde sea necesario un suministro continuo y fiable de gas.

www.sick.com

Bornas de medición con tecnología Push-X

■ Phoenix Contact presenta sus nuevas bornas de medición XTVMEA 6 que destacan por el cortocircuito automático adelantado del transformador de corriente. Esta función make before break permite un funcionamiento seguro del transformador de corriente para todas las tareas de mantenimiento y ensayo. Estas nuevas bornas de medición están equipadas con tecnología de conexión Push-X, que no requiere fuerza ni herramientas, y es una de las tecnologías de conexión más rápidas y flexibles, ya que se adapta a todo tipo de conductores, con o sin punteras. Gracias a la conexión de conductores lateral, las bornas ofrecen marcas de conexión grandes y fáciles de leer. El sector energético, en particular, se beneficia de las bornas de medición XTVMEA 6. Son adecuadas para todas las aplicaciones de medición y protección. Totalmente compatibles con la serie de bornas ME 6 existente de Phoenix Contact. Tienen un diseño ergonómico y dos veces tres fosos puenteados. También se pueden utilizar los accesorios del sistema CLIPLINE complete. Hay nuevos accesorios adicionales para realizar un cortocircuito. Con la palanca de mando C-MEA... y los puentes multipolo enchufables SB-MEA... se pueden accionar y cortocircuitar varias bornas simultáneamente. La serie XTVMEA 6 se completa con bornas de paso y bornas de tierra con el mismo contorno.



www.phoenixcontact.com

Convertidor matricial U1000

■ El convertidor matricial U1000 de Yaskawa es un convertidor de CA altamente eficiente que puede utilizarse para accionar máquinas síncronas o asíncronas, con o sin codificador, a la vez que realimenta la energía que genera. Los modelos de la serie cubren una amplia gama de potencias de 2,2 a 500 kW. A diferencia de las soluciones de energía regenerativa tradicionales, el U1000 no tiene bus de CC, sino que conmuta la energía trifásica de la red directamente a las bobinas del motor. Los flujos de potencia del U1000 son prácticamente sinusoidales, independientemente de si funciona en modo motorizado o regenerativo. Esto representa un potencial de ahorro energético excepcional, especialmente en Alemania, donde los costes de la electricidad se encuentran entre los más altos del mundo. La energía devuelta por un sistema regenerativo puede utilizarse internamente en plantas industriales. Cuando se trata de reducir los costes de electricidad, el modo ECO (bypass electrónico) del convertidor lo hace destacar sobre el resto. Gracias a su innovador diseño (sin bus de CC interno), el U1000 puede conmutar la tensión de red a la salida 1:1 cuando funciona a frecuencias de red (50 Hz en Europa o 60 Hz en EE.UU./Japón). No es necesario conmutar los IGBT en este estado, por lo que se puede ahorrar hasta un 300% de la potencia potencial perdida, en comparación con los productos de la competencia.



www.yaskawa.es

PRÓXIMO NÚMERO



SECTOR

Naval

TECNOLOGÍA

Sensórica virtual

INFORME

AMR's (Robots autónomos móviles)

SÍGUENOS...

...conversa
con nosotros
sobre la actualidad
de tu sector



Seguro, preciso y versátil

D-Bot: listo en menos de 3 horas



D-Bot



reddot winner 2024
best of the best

Colabora con el Cobot Delta: tu mejor aliado para la automatización

- Carga útil: de 6 a 30 kg
- Alcance: de 800 a 1.800 mm
- Montaje omnidireccional
- Clasificación IP66: protección contra el agua y el polvo
- Máxima precisión: margen de repetibilidad de $\pm 0,02$ mm

Delta Electronics Solutions (Spain) S.L.U.
Sales.IA.Iberia@deltaww.com
www.delta-emea.com





20 & 21
noviembre 2024
IFEMA



The future of
advanced materials
and manufacturing
technologies.

**REGÍSTRATE
GRATIS ONLINE**



CÓDIGO: 20100

 advancedmanufacturingmadrid.com

 ammadrid@easyfairs.com

 +34 91 541 24 88

by **EASYFAIRS**

 **advanced manufacturing**
madrid24

Platinum Sponsor



Gold Sponsors

